

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers — the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee — meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmsdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.