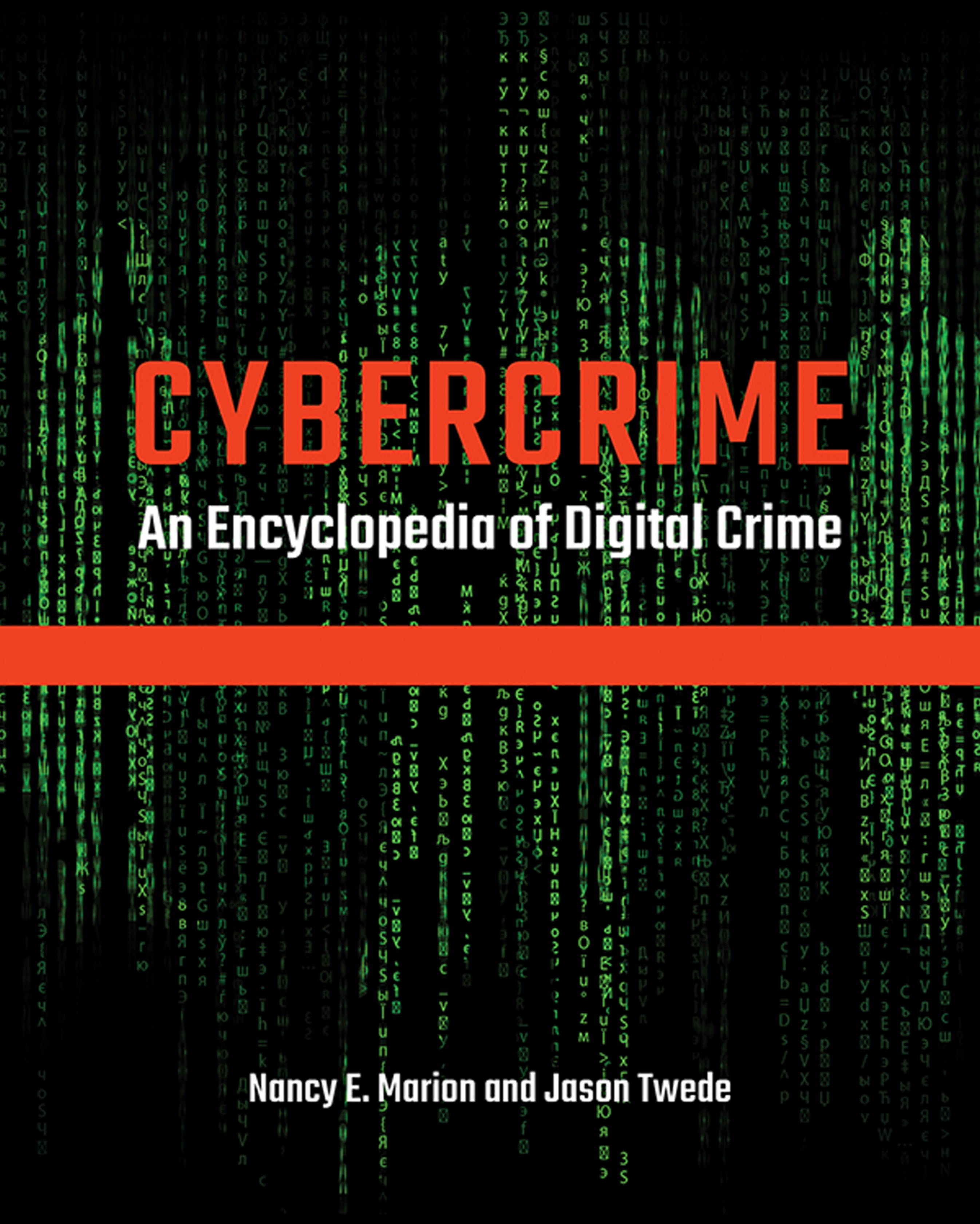

CYBERCRIME

An Encyclopedia of Digital Crime

Nancy E. Marion and Jason Twede

Cybercrime

Cybercrime

An Encyclopedia of Digital Crime

NANCY E. MARION AND JASON TWEDE

ABC-CLIO®

An Imprint of ABC-CLIO, LLC
Santa Barbara, California • Denver, Colorado

Library of Congress Cataloging-in-Publication Data

Names: Marion, Nancy E., author. | Twede, Jason, author.
Title: Cybercrime : an encyclopedia of digital crime / Nancy E. Marion and Jason Twede.
Description: First Edition. | Santa Barbara : ABC-CLIO, 2020. | Includes bibliographical references and index.
Identifiers: LCCN 2019056395 (print) | LCCN 2019056396 (ebook) | ISBN 9781440857348 (hardcover) | ISBN 9781440857355 (ebook)
Subjects: LCSH: Computer crimes. | Computer crimes—Prevention.
Classification: LCC HV6773 .M372 2020 (print) | LCC HV6773 (ebook) | DDC 364.16/803—dc23
LC record available at https://lccn.loc.gov/2019056395
LC ebook record available at https://lccn.loc.gov/2019056396

ISBN: 978-1-4408-5734-8 (print)
978-1-4408-5735-5 (ebook)

24 23 22 21 20 1 2 3 4 5

This book is also available as an eBook.

ABC-CLIO
An Imprint of ABC-CLIO, LLC

ABC-CLIO, LLC
147 Castilian Drive
Santa Barbara, California 93117
www.abc-clio.com

This book is printed on acid-free paper ∞

Manufactured in the United States of America

Contents

List of Entries

Introduction

There is no single, conclusive definition of the term “cybercrime”; however, it has become an umbrella term that refers to a wide range of offenses and behaviors. Other terms that are also used are computer crime, computer-related crime, virtual crime, digital crime, e-crime, high-tech crime, electronic crime, cyber-enabled crime, or even online offending. In general, it refers to any criminal offenses that are committed or aided by use of the internet. It is difficult to provide an exact definition of cybercrime because it is always changing and evolving as technology advances and becomes more sophisticated.

Some define cybercrime as any crime that involves a computer or a network. Sometimes the computers are used to commit the crime, but other times they are the target of the crime. According to the U.S. Department of Justice, the term “cybercrime” refers to any illegal activity for which a computer is used as its primary means of commission, transmission, or storage.

Some definitions of the term make a distinction between cybercrime and computer crimes. Those who make this difference describe cybercrime as those offenses in which the offender obtains special of cyberspace and relies on that knowledge to carry out a criminal offense. This would happen, for example, if a person hacked into another person’s account and accessed private photos of them and then uploaded the photos to social media. On the other hand, computer crimes can be thought of as those times when an offender uses special knowledge about computer technology to commit a crime. An example is when a person uses a computer to download confidential information onto a zip drive and removes it from that source. They are using a computer to commit a crime—but not the internet. In short, one offender relies on the larger concept of cyberspace whereas the other relies on the more hands-on offenses committed by the use of tangible items (software or computer equipment) (Holt, Burruss, and Bossler, 2015, p. 7).

There are other distinctive definitions of specific cybercrimes. One of those is a computer-assisted crime, such as child pornography. Here, the offender uses the computer to commit the crime. They will use the computer to create the illegal material (virtual pornography) and then to distribute it. A computer-focused offense is one in which the computer is an essential part of the offense, such as hacking into an account. This offense could not be carried out without the computer.

Wall (2001) recognizes four categories of cybercrime. The first is cybertrespass, which he defines as those times when an offender crosses the undefined or invisible but often recognized lines of ownership in an online environment. This occurs when hackers steal passwords and obtain access to resources for their own benefit. They have used the online environment (the internet) to steal something that belongs to another person. The second category includes cyberdeception and cybertheft. This involves the use of computers to steal money from bank accounts or to illegally access intellectual property or copyrighted material (music, movies, books, software) from another person. This is also referred to as piracy. Cyberdeception occurs through phishing, when a cybercriminal sends a sham e-mail to a victim asking for bank account information. Because the e-mail appears to be real, the victim provides the information. The stolen information can be used by the offender to steal money, or it can be sold to other offenders.

The third category of cybercrime, according to Wall, is cyberpornography and obscenity. Internet and computer technology allow pedophiles to create and trade graphic pictures or meet victims. The final category of cybercrime is cyberviolence, which is hurtful or dangerous behavior committed online. Computers give offenders the ability to create and distribute threatening and hurtful information about others. Examples of these offenses include cyberharassment, cyberstalking, and cyberbullying.

It is difficult to list all of the cybercrimes that exist, as there are many different kinds of cybercrimes. Many cybercrimes were considered to be criminal offenses prior to the evolution of the internet (e.g., bullying, child pornography, or theft) but have evolved into a cybercrime; others are new offenses that did not exist before (e.g., hacking or sexting). Below is a partial list of offenses that are often committed in cyberspace or by use of a computer.

(a) Ransomware: Malware used by offenders to lock digital files of another person or company until money or other form of ransom is paid to the offender.

(b) Phishing: A way for criminals to obtain private information from a victim by sending an e-mail that appears to be from a legitimate organization. The e-mail often uses letterhead from the agency or a logo from the company to make it look real. The message indicates that an account or password needs to be updated. The victim is tricked into providing that information to the offender, who then uses it to steal the victim's money or sells the information to another offender.

(c) Identity theft: A criminal obtains a victim's personal information (possibly through phishing) and uses that to commit theft or fraud offenses, open fake credit card accounts, or get bank loans. They use a victim's name, birthday, social security number, driver's license number, or passport information. A victim of identity theft can suffer extreme and long-lasting financial harm. This offense is not punishable under the federal Identity Theft and Assumption Deterrence Act of 1998, which "makes it a federal offense to possess, transfer or use a means of identification of another person without authorization with the intent to commit or aid in the commission of illegal activity at the local, state or federal level."

(d) Online child predators (child pornography): This offense has been defined as "the sexual or sexualized physical abuse of children under 16 years of age or who appear to be less than 16 that would offend a reasonable adult" (Krone, 2004, p. 1). Images of child pornography show children participating in sexual acts. Children who are forced into participating in the acts suffer trauma and are often permanently injured, both physically and emotionally. The production and consumption of child pornography are both illegal acts, regardless of whether the computer is involved. The internet allows people to access child pornography for free, but there are multiple sites on the dark web that make these images readily available. It is estimated that there are 20,000 images of child pornography added to the internet each week (Pittaro, 2008). Because of the sheer amount of child pornography available on the internet, law enforcement has a difficult time tracking users. It is easy for offenders to skirt the law and get away with this offense.

(e) Viruses: A form of malware, viruses are computer programs that a user unknowingly uploads onto their computer when they open an infected e-mail or attachment, or when they visit a particular website. The virus is uploaded onto the computer, giving the offender access to the files on that machine. The virus allows the offender to steal data, destroy data, or access personal information. It will then replicate itself onto other computers through e-mails.

(f) Denial-of-service attacks (DoS attacks): These attacks are carried out by cybercriminals who block or prevent a legitimate user from using a website. Offenders are able to flood a computer network with enough traffic that the site crashes, shutting it down to other users. This type of attack can result in significant losses to the company as they must spend time and resources to get their site working once again. A similar attack is a distributed denial-of-service attack (DDoS) that occurs when a site is overwhelmed by botnets (a group of infected computers and networks) that overwhelm a targeted website with requests and render the site or servers unavailable to users.

(g) Malware: This term is a combination of the words "malicious" and "software." It refers to any software that has the intent of harming networks or devices or giving an offender unauthorized access to computers or networks belonging to another person or organization. It is usually uploaded onto a victim's computer or network without their knowledge and may remain there for an extended time. Types of malware include viruses, spyware, worms, ransomware, adware, and Trojan horses.

(h) Cyberbullying: This occurs when a person harasses or teases another person, usually a teenager, through social media. It can be relentless and extremely harmful, and it has led some victims to commit suicide. When this behavior is directed toward an adult, it is called cyberharassment.

(i) Cyberterrorism: According to the FBI, cyberterrorism involves crimes of terrorism that occur electronically or through the use of the internet. They can be directed against individuals, businesses, agencies, and the government. It can be acts on the internet that are meant to threaten or extort others, often politically motivated. If an attack is carried out, it can cause disruption of services that may be harmful or even cause death.

(j) Hacking: Illegally breaching security or gaining access to a computer system by an offender who is called a hacker. Some hackers intend to do harm, either by stealing money or information, whereas others hack into a system as a way to uncover unknown weaknesses or vulnerabilities in software.

(k) Piracy: The unauthorized copy and distribution of movies, music, or other copyrighted property without permission of the owner or creator. This can happen when a person downloads a program, video game, or a song without paying for it.

(l) Spyware: A type of malware that can be secretly installed in a victim's computer to allow an offender to steal a victim's information. An offender is able to steal passwords, e-mails, and credit card information without the victim knowing.

(m) Nigerian e-mail schemes: These are also known as advance fee e-mail schemes. Here, the victim receives an e-mail pleading for money to be sent somewhere, with promises that more money will be provided in the future. They often appear to be from an official or member of royalty who needs help to leave their country. The offender will request the bank account number where the promised money can be sent. The scams often originate in Nigeria but are also called 419 scams after the Nigerian statute that bans this kind of communication.

(n) Work-at-home schemes: These often involve job solicitations where the victim is given the chance to work at home completing menial tasks (stuffing envelopes) and earn a significant income for only a few hours of work each day. The victim is required to pay up-front for training materials or supplies, but materials are never sent.

(o) Romance schemes: A victim meets their perfect romantic partner through an online dating site. The offender will ask for money to travel and meet their new soul mate, to pay get out of legal trouble, or to pay off debts. They may initially ask for a small amount, but then it increases over time. Victims have paid tens of thousands of dollars before realizing their new mate doesn't exist.

However you define it, cybercrime costs billions of dollars to companies, governments, and individuals in financial losses of information and trade secrets. Losses are also due to repairs to systems that are damaged or harmed as the result of a cyberattack. Individuals, governments, and agencies must also spend billions in prevention of a possible attack.

Cybercrime poses a threat to our country's national security and infrastructure. Other governments and terrorist organizations have threatened to attack the infrastructure of the United States (power grids and financial institutions). The U.S. government spends billions of dollars each year to thwart possible attacks on its agencies, as well as to keep citizens safe. It is an ongoing process that must evolve as threats evolve.

Cybercrime is difficult to combat for many reasons. One is that cybercriminals do not respect physical boundaries. The internet is a global phenomenon that crosses borders, and so is cybercrime. This makes it difficult for law enforcement to track. It is difficult to know who the offender is or where that person is physically located. Investigating cybercrime requires offices to have knowledge of technical forensic methods, which few do. To effectively battle cybercriminals, there must be cooperation on an international level. Interpol currently helps to fight cybercrime, but more needs to be done. Because it is so tough to track, there is a relatively low risk of detection and prosecution to offenders.

In the United States, the Federal Bureau of Investigation (FBI) is the primary federal agency that has the responsibility to investigate any threat of, or actual events of, cybercrime. They have a cyber division that coordinates the nation's attack on cybercrime. Each field office has a cyber squad comprising specially trained agents who work to protect against crimes and also to react to attacks. The FBI has formed cyber action teams that respond worldwide to an attack to gather intelligence and work to identify the crime and criminals. The FBI has created 93 computer crimes task forces that work with state and local experts in the fight against cybercrime. They also partner with other federal agencies, including the Department of Defense, Department of Homeland Security, and others. The FBI's Internet Crime Complaint Center gives the public a way to report acts of cybercrime.

Cybercrimes such as these are often committed by criminals who are seeking to profit from their crimes. They hack into an account to get money, or use ransomware for the same reason. Cybercrimes are committed by terrorists who are seeking to intimidate others, or even to profit from their crimes. Hackers sometimes commit cybercrimes just for the challenge, or to see if they can break into a system. The internet gives offenders the chance to harm many people at one time, something that might not be possible without using a computer. There is a large pool of victims available to the offender. It is also an inexpensive way to commit a crime. In some cases, all it takes to scam a victim is to send an e-mail. There is a large amount of malware that offenders can purchase that allows them to carry out an attack even though they have no expertise in writing software.

Cybercrimes are growing as more people have access to computers and rely on them for daily tasks such as shopping, banking, and communicating with each other. The true range of cybercrime is unknown, as many people do not report when they have been a victim, or they may not even know that they have been attacked. Businesses may not want to make it known to their customers that they have been the victim of a cybercrime and risk harming their reputation. Threats to mobile devices are also on the rise as people use them as computers, keeping personal information, contacts and calendars on them. Both individuals and companies need to become more aware of how to protect themselves from cybercrime. It can be as simple as purchasing programs that will protect against viruses and malware—or using passwords that are difficult to hack. Teaching employees and individuals to recognize fake e-mails is also critical, so they do not fall prey to cybercriminals who only want to have access to bank accounts.

Nancy E. Marion

Further Reading

Clough, Jonathan. 2015. *Principles of cybercrime*. Cambridge, UK: Cambridge University Press.

Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). https://www.ic3.gov

Finch, Emily. 2007. "The problem of stolen identity and the internet." In *Crime online*, edited by Yvonne Jewkes. Devon, UK: Willan Publishing, pp. 29–43.

Gillespie, Alisdair A. 2016. *Cybercrime: Key issues and debates*. New York: Routledge.

Holt, Thomas J., George W. Burruss, and Adam M. Bossler. 2015. *Policing cybercrime and cyberterror*. Durham, NC: Carolina Academic Press.

Hutchings, Alice, and Yi Ting Chua. 2017. "Gendering cybercrime." In *Cybercrime through an interdisciplinary lens*, edited by Thomas J. Holt. New York: Routledge, pp. 167–188.

Krone, T. 2004. "A typology and online child pornography offending." *Trends and Issues in Crime and Criminal Justice* 279: 2–6.

Lininger, Rachael, and Russell Dean Vines. 2005. *Phishing*. Indianapolis, IN: Wiley Publishing.

Pittaro, M. 2008. "Sexual addiction to the internet: From curiosity to compulsive behavior." In *Crimes of the internet*, edited by F. Schmalleger and M. Pittaro. Upper Saddle River, NJ: Pearson Education, Inc., pp. 134–150.

Wall, D. S. 2001. "Cybercrimes and the internet." In *Crime and the internet*, edited by D. S. Wall. New York: Routledge, pp. 1–17.

Chronology

May 29, 1864 Dentist Messrs Gabriel sends an unsolicited telegraph for his dentistry to British politicians, advertising his hours of operation. This is seen as the first example of spam.

June 4, 1903 Nevil Maskelyne, a magician and inventor, disrupts the public demonstration of Guglielmo Marconi's wireless telegraphy technology to the Royal Institution in London by John Ambrose Fleming. Marconi claimed the wireless telegraph technology was secure. Maskelyne was able to break into the supposedly secure system and sent trolling Morse Code messages over the line during the presentation. This is viewed as the first instance of hacking.

July 26, 1908 The FBI (originally known as just the Bureau of Investigation) is created.

April 5, 1955 The minutes of a meeting of the Tech Model Railroad Club at the Massachusetts Institute of Technology (MIT) use the term "hacking" in reference to those experimenting or otherwise goofing around with technology. This is the first known recorded instance of the term "hacking" being used in this fashion.

1957 Josef Engressia (also known as Joybubbles), a seven-year-old boy who is blind, discovers that if he whistles a specific note (the fourth E above middle C), he is able to access the telephone system of AT&T. This discovery paves the way for phreaking.

November 20, 1963 *The Tech*, the student newspaper at the Massachusetts Institute of Technology (MIT), uses the term "hacker" in reference to students who were disrupting phone services at the school and avoiding long-distance phone charges, in some instances routing charges to a third party. This is the first known recorded instance of the term "hacker" being used pejoratively to refer to those who use technology in an unauthorized manner with apparent malicious intent.

November 15, 1968
Josef Engressia (also known as Joybubbles) is suspended from the University of South Florida for obtaining free phone calls for classmates by whistling a specific tone at different intervals into the phone. The suspension was later rescinded, and he was placed on probation at the school.

October 1, 1971
Esquire magazine publishes an article about blue box phone phreaking. The article features John Draper (also known as Captain Crunch) and Josef Engressia (also known as Joybubbles). Draper is only referred to by his alias in the article.

1971
The Creeper virus spreads through ARPANET, the precursor of the internet. The Creeper virus is generally regarded as the first computer virus.

June, 1974
The term "Trojan horse" is first used in a vulnerability analysis report published by the U.S. Air Force.

May 1, 1978
Gary Thuerk sends several hundred unsolicited advertisements to recipients via ARPANET, a computer network used by the U.S. military that predated the internet. This is regarded as the first instance of modern spam.

1978
The Florida legislature passes the Florida Computer Crime Act, one of the first laws to establish parameters that defined computer crimes.

1979
Kevin Mitnick hacks into his first computer system, the Ark.

1981
Ian Murphy, AKA Captain Zap, is able to break into the computer system of AT&T and change the internal clock. This allows callers to receive the "late-night" discount rate in the middle of the day. Murphy becomes the first person ever convicted of a computer crime.

1981
The movie *Sneakers* is released, based on Captain Zap's hacking experiences.

1981
The Chaos Computer Club forms in Germany.

1982
The hacking group 414s is formed in Milwaukee, Wisconsin, naming themselves after the city's telephone area code. The members are able to access the nuclear weapons laboratory of the Los Alamos National Laboratory and the Sloan-Kettering Cancer Center in New York, among other high-profile sites.

1983
The movie *War Games* is released. The movie introduces the concept of hacking and shows the public the potential dangers of hacking.

1983	Members of a hacking group, the 414s, break into 60 computer systems at various institutions, including Sloan-Kettering Cancer Center and the Los Alamos National Laboratory. The incident made people aware of the dangers of hacking. The U.S. House of Representatives holds hearings on computer security and passed several new laws to deter hacking.
February 1983	The group KILOBAUD is formed, motivating other groups to form.
1984	The hacking group Legions of Doom is formed by a hacker known as Lex Luthor.
1984	Cult of the Dead Cow forms in Lubbock, Texas.
1984	The hacker magazine *2600* is published for the first time. It is known for articles that describe tips on hacking and phone phreaking.
1984	The Chaos Computer Club organizes the Chaos Communication Congress, an annual hacker conference.
1985	First issue of Phrack is published. It becomes the magazine for underground hackers.
1986	The U.S. Congress passes the Federal Computer Fraud and Abuse Act that makes it a crime to break into federal computers.
1986	Pakistani Brain, the oldest known and recognized virus, is discovered to infect IBM Computers.
1986	The hacker known as "The Mentor" is arrested and composes the Hacker's Manifesto in the magazine *Phrak*.
1987	The Jerusalem Virus that infected on Friday the 13th is discovered. It was one of the first file-infecting viruses.
1987	The Christmas Tree EXEC "worm" causes major disruption to the VNET, BITNET, and EARN networks.
1988	Robert Morris, a Graduate Student at Cornell University, releases the Morris worm, the first internet worm that spreads to 6,000 networked computers, shutting down the internet. He is later convicted and sentenced to three years of probation and fined $10,000.
1988	The First National Bank of Chicago is the victim of a hacking that resulted in the theft of $70 million.
1988	The Computer Emergency Response Team (CERT) is created by DARPA to focus on network security issues.
1988	Kevin Mitnick is sentenced to a year in jail for hacking the network of the Digital Equipment Company.

1989 The hacking magazine *Phrak* publishes a confidential document from Bell South that was obtained illegally by hackers.

1990 Hacker Kevin Poulsen is arrested after gaining access to the telephone lines for a radio station in Los Angeles so he could win a Porsche and other prizes.

1990 The war between rival hacking groups, Legion of Doom (LOD) and Masters of Deception (MOD), begins.

1990 Operation Sundevil is completed by the Secret Service as agents arrest hackers, including prominent members of the Legion of Doom. The offices of Steve Jackson Games are also part of the raid. The role-playing sourcebook GURPS Cyberpunk is seized by law enforcement because, as they describe, the book is a handbook for computer crime. Hackers begin to inform on each other as a way to receive lighter sentences.

1990 Birth of spam.

1990 The Electronic Frontier is founded.

1991 The virus called "Michelangelo" appears in computers. The malware attacks PCs and is programmed to destroy hard drives on Michelangelo's birthday, March 6.

1991 Kevin Poulsen, also known as Dark Dante, is captured by the FBI. He pleads guilty to charges of mail, wire, and computer fraud and is sentenced to a term of 51 months in prison and is also required to pay a fine of $56,000.

1991 Dark Avenger writes and releases MtE, malware that allows other viruses to morph into an estimated four billion forms. This makes both detection of the virus and its deletion more difficult.

June 5, 1991 Philip Zimmermann releases Pretty Good Privacy (e-mail encryption software). It is released as freeware.

1992 Dark Avenger writes and launches a virus called Commander Bomber that is especially harmful because it remains undetected in a computer's memory and can change form. Other malware released this year were SatanBug and Monkey.

1992 The movie *Sneakers* is released. The primary characters in the film are security experts who are tricked into stealing a universal decoder to unlock encryption systems.

June 1993 First DEF CON hacker convention meets in Las Vegas, Nevada. This becomes a yearly event attended by thousands of people from around the world.

1993 The term “spam” is first associated with unsolicited electronic communications. This was in response to hundreds of copies of the same message being accidentally posted to a website.

1994 The FBI launches Operation Innocent Images. FBI agents pose undercover to investigate child pornographers and pedophiles.

1994 Russian computer hacker Vladimir Levin, 30 years old, is able to gain access into the computer system of Citibank. He then transfers $10 million of other people’s money into his personal account. Levin is later arrested in London and charged with criminal offenses in the United States. He is convicted and sentenced to three years in prison. Most of the transferred money is eventually recovered.

1994 Mark Abene, also called “Phiber Optik,” is sent to jail for tampering with telephone lines. Before being sent to prison, he is a member of the hacker gang Masters of Deception. Abene is later named one of New York City’s smartest people.

1995 Hacker Kevin Mitnick is arrested and charged by the FBI with stealing 20,000 credit card numbers.

1995 The movies *THe Net* and *Hackers* are released. *THe Net* is about a computer analyst who is able to access classified documents and becomes involved in a conspiracy. *Hackers* is about high school students who become hackers.

1996 Computer malware called Concept is released. It was spread through emails and affected both Macs and PCs.

1996 Hackers are able to access and alter the web sites belonging to the U.S. Department of Justice, the CIA, and the U.S. Air Force. This brings attention to the need for tighter security for the internet.

1996 U.S. Congress passes the Computer Fraud and Abuse Act. The law bans the dissemination of malware and trafficking in computer passwords.

January 11, 1996 The investigation by the U.S. government into Philip Zimmermann is closed without criminal charges being filed. The government is investigating whether Zimmermann’s distribution of encryption software Pretty Good Privacy violated the law by being available in foreign countries.

1997 Six Degrees, the first social media platform, is launched.

1997 A 15-year-old boy living in Croatia is able to access the computer system of the U.S. Air Force base in Guam.

1997 The interest group Recording Industry Association of America begins to crack down on the practice of file sharing and peer-to-peer networks.

October 28, 1998 The U.S. Digital Millennium Copyright Act is passed by the U.S. Congress.

1998 Members of a LOpht, a "hacker think tank," answers questions in front of the U.S. Congress. They were invited to speak in front of the Government Affairs Committee about the need for stronger security for government sites.

1998 The hacking group Cult of the Dead Cow (cDc) develops a Trojan horse they called Back Orifice.

1998 The websites of the U.S. military and Department of Defense continues to be hacked. The *New York Times* is also accessed by cyberoffenders.

1998 The National Infrastructure Protection Center is established by Attorney General Janet Reno. The organization is given the task of fighting cybercrime and possible sabotage of U.S. businesses.

1998 A reporter for the *Cincinnati Enquirer*, Michael Gallagher, is able to access the voice mail system at Chiquita Fruits. Officials at the newspaper opt to publish illegal activities carried out by employees of Chiquita.

1998 A cybercriminal uses social engineering to convince a staff member at AOL to provide access to the ACLU's website. The offender wipes out all of the information on the site.

1999 President Bill Clinton announces that he will allocate $1.46 billion to improve the nation's cybersecurity. He proposes an "intrusion detection" system to discover cyberattacks.

1999 The hacking group Cult of the Dead Cow, cDc, releases the second version of Back Orifice, BO2k. This version is more powerful than the first and becomes popular among hackers.

1999 Hackers in Serbia and Kosovo attack each other through the government's websites.

1999 Two hackers from China access financial records for a bank and transfer about $87,000 into their accounts. They are later found guilty and sentenced to death.

1999 A number of well-known viruses are released this year. One is the Melissa virus, which modifies a victim's documents and/or sent out confidential information, causing over $80 million in damages. Another virus is Chernobyl, which can remain undetected but, when activated, will erase data on a user's hard drive. The virus Thursday applies itself on a specific date chosen by the offender. When activated, this virus releases all files. Bubble Boy is spread through e-mail script, so it does not require a user to open an infected attachment.

1999 The site for the U.S. White House is vandalized. Those accessing the site see "Hacker wuz Here" in red graffiti.

1999 A black-hat hacking group called "phreak.nl" is able to damage many high-profile websites such as NASA and the National Defense University. The members explain that the hacking was part of a game called "Hack the Planet."

1999 Hacker Kevin Mitnick is found guilty and sentenced to spend five years in prison. He had already spent four years in custody prior to the trial, including eight months in solitary confinement because officials thought he could cause great harm to the nation by his hacking activities.

1999 Members of a hacking group called Level Seven Crew access the website belonging to the U.S. Embassy in China and place antigovernment statements on the site.

1999 Hacker Michael Calce, who went by the moniker Mafia Boy, carries out attacks on Yahoo, Amazon, Dell, eBay, and CNN, causing $1.7 billion in damages.

March 26, 1999 The Melissa virus is released by David Lee Smith. It is one of the first viruses to utilize mass e-mailing to spread.

April 1, 1999 David Lee Smith is arrested for releasing the Melissa virus.

November 29, 1999 The Anticybersquatting Consumer Protection Act takes effect in the United States.

May 8, 2000 The Internet Crime Complaint Center (originally known as the Internet Fraud Complaint Center) is founded.

May 9, 2000 Timothy Lloyd is convicted for using malware to destroy the manufacturing abilities of his former employer, Omega Engineering Corporation. He uses a logic bomb to carry out the crime.

2000 The Center for Internet Security is formed.

2000 The ILOVEYOU virus infects millions of computers around the world quickly. It originates in the Philippines.

2000 Computer hacker Jonathan James is the first juvenile sentenced to serve time in a facility for hacking.

December 3, 2001 In the wake of 9/11, the FBI announces the creation of a cyber division.

2001	The “Anna Kournikova” virus is launched. The e-mail tempts people to open an attachment that has pictures of the tennis player. When people open the attachment to view the photos, the virus is attached.
2001	The Code Red worm is launched and infected thousands of computers around the world.
February 26, 2002	Timothy Lloyd is sentenced to 41 months in prison for using malware to destroy the manufacturing abilities of his former employer, Omega Engineering Corporation. His conviction is set aside by the trial judge, though he was ultimately reinstated by an appellate court.
September 20, 2002	The initial version of Tor (The Onion Router) is launched.
2002	Bill Gates announces that he is increasing security for Microsoft products.
2003	The hacking group Anonymous is formed.
2003	A piece of federal legislation, called the CAN-SPAM Act, is passed by the U.S. Congress. The bill put limits on how much unsolicited spam e-mail can be sent.
2003	Einstein is created by the Department of Homeland Security to detect cyberattacks.
August 11, 2003	Blaster worm is released.
August 18, 2003	Welchia worm is released to combat the Blaster worm.
February 6, 2004	The first Safer Internet is celebrated. Fourteen countries are involved in the celebration.
2006	Wikileaks is founded.
October 3, 2006	The first International Day against DRM is sponsored by the Defective by Design organization.
2006	Operation Olympic Games/Stuxnet is announced.
2007	A spear phishing attack launched against the U.S. Secretary of Defense allows cybercriminals to have access to sensitive information. Officials decide to make significant changes to secure their information.
2007	An “advanced persistent threat” attack, called Ghost Net, is launched. Some allege the attack is carried out by the People’s Republic of China.
January 21, 2008	The hacking group Anonymous launches Project Chanology (or Operation Chanology), a protest movement against the Church of Scientology. A few days later, on January 24, members of Anonymous take the website Scientology.org offline.

2008 Hackers from China report that they have accessed some of the world's most sensitive sites, including the Pentagon.

2008 The computer worm Koobface is detected.

2009 Bitcoin is created by Satoshi Nakamoto. Nakamoto sends the first Bitcoins to Hal Finney.

2009 Phillip Markoff carries out the Craigslist killings, in which he kills women he meets through the website.

2009 Over 100 people are charged in the United States and around the globe in an investigation into cybercrimes through Operation Phish Phry.

2009 Operation Aurora is launched to investigate cyberattacks that are carried out to access sensitive and personal data.

January 25, 2010 Brian Mettenbrink, an engineering student and supporter of Anonymous, pleads guilty to downloading LOIC to attack Scientology. He is sentenced to one year in prison.

April 5, 2010 Wikileaks releases footage of U.S. military helicopters killing several people in Iraq. Among those killed are journalists.

May 22, 2010 The first commercial Bitcoin takes place. Laszlo Hanyecz of Florida pays 10,000 Bitcoins to an individual from the United Kingdom for two pizzas from Papa John's.

July 6, 2010 Private Chelsea Manning is charged with disclosing video footage of U.S. military helicopters killing people in Iraq, including journalists.

September 17, 2010 Anonymous attacks Aiplex Software after it admits to launching an attack on the Pirate Bay. Anonymous also launches attacks on the Motion Picture Association of America, Recording Industry Association of America, and law firms that oppose internet piracy.

2010 The banking Trojan Carberp appears.

2010 Stuxnet worm, a cyberattack on Iran's nuclear facilities allegedly conducted by the U.S. and Israel, appears on the internet.

December 2, 2010 PayPal announces that it will no longer fund WikiLeaks.

December 8, 2010 Julian Assange surrenders to law enforcement in the U.K. in regard to a warrant for criminal charges out of Sweden.

December 8–9, 2010 Anonymous attacks PayPal for its opposition to WikiLeaks in Operation Avenge Assange, bringing down the site.

December 16, 2010 Julian Assange is given bail in the United Kingdom in the amount of £240,000. Supporters of Assange are able to gather the full amount of bail, and Assange is released from custody while his extradition case is pending.

2010	Hacking group Goatse Security hacks into the computer system belonging to AT&T and then uploads the names and e-mail addresses of 114,000 iPad users.
2010	A form of malware called "Carberp" attacks online banking and social media sites. Cybercriminals use it to steal millions of dollars from banks in Russia.
2010	Sam Yin, a computer expert for Gucci, is fired from his job and then accesses the company's computer system to shut it down for a day. After pleading guilty, he is sentenced to two to six years in prison.
February 2011	Silk Road founded.
February 6, 2011	Anonymous allegedly steals thousands of corporate e-mails from Aaron Burr's e-mail account. They also take over his Twitter account and deface his company's website.
February 24, 2011	Anonymous conducts a live hack of a website of the Westboro Baptist Church.
April 1, 2011	Anonymous members initiate a DDoS attack on Sony websites and Sony PlayStation, to the dismay of gamers.
April 7, 2011	Anonymous stops the attack on SONY because they do not want to further disrupt the PlayStation network, but it remains offline for the next few weeks.
April 23, 2011	One of the last known communications of Satoshi Nakamoto—the creator of Bitcoin—is made to Bitcoin developer Mike Hearn via e-mail. Nakamoto says, "I've moved on to other things. It's in good hands. . . ."
May 25, 2011	China announces the creation of a cyberdefense squad with the People's Liberation Army.
July 19, 2011	British police arrest a 16-year-old whom they claim is a hacker with LulzSec known as Tflow.
July 27, 2011	Police arrest Jake Davis, whom they claim is Topiary in LulzSec.
September 2, 2011	Police in Britain arrest Ryan Ackroyd, 24 years old, who was Kayla in LulzSec.
2011	The hacker group Lulz Security is formed by breaking away from Anonymous.
2011	The website for the Bank of America is hacked and information from an estimated 85,000 credit card numbers and accounts are reportedly stolen.
2011	A hacking attack takes the PlayStation Network offline and compromises credit card information and other personally identifying information of 77 million customers.

2011 The YouTube channel presenting Sesame Street, an educational show for children, was hacked so that the station showed pornographic images for almost 22 minutes.

2011 Christopher Chaney is arrested for hacking into the e-mail accounts of celebrities, stealing photos and other information and posting them online.

2011 Brian Rafferty and Richard Beasley kill men who applied for a job posted on Craigslist.

June 19, 2012 Assange takes up residency at the Ecuadoran embassy.

August 16, 2012 Ecuador grants asylum to Assange amid concerns that his extradition may result in the infringement of his human rights.

November 2012 Andrew Auernheimer is found guilty of one count of identity theft fraud and one count of conspiracy to access a computer without authorization.

2012 Iranian hackers retaliate against Stuxnet by releasing Shamoon, a virus that damages 35,000 Saudi AramCo computers and stops the company for a week.

2012 Marriott is hacked by a New Age ideologist who was resisting against the New World Order where he said that corporations are controlling the world.

2012 The social networking website LinkedIn is hacked, and passwords for nearly 6.5 million user accounts are stolen.

2012 Ryan Cleary, a member of LulzSec, is arrested for hacking activities. He is able to access the websites of the CIA, the Pentagon, SONY, Nintendo, the Westboro Baptist Church, and many other companies. He is later sentenced to serve 32 months in prison.

2012 The U.S. Congress passes the Cybersecurity Act of 2012 to enhance the security of the nation's cyberstructure.

June 2013 Banking Trojan Carberp is leaked, leading to fears of copycat offenses.

August 21, 2013 Chelsea Manning is sentenced for her convictions on criminal charges stemming from her release of information to WikiLeaks regarding the U.S. wars in Iraq and Afghanistan. She receives a sentence of 35 years in prison.

October 2013 Silk Road shut down by the FBI.

2013 North Korea allegedly disrupts the financial institutions in South Korea using a program called "DarkSeoul."

2013 Twelve-year-old Rebecca Sedwick commits suicide after being bullied on social media.

2013	The European Cybercrime Center, or EC3, is formed by Europol to increase law enforcement response to cybercrime.
2013	The National Cybersecurity and Critical Infrastructure Protection Act is passed by U.S. Congress and signed into law.
2013	Sunil Tripathi, a student at Brown University, is wrongly doxed as one of the suspects in the Boston Marathon bombing.
February 25, 2014	Mt. Gox goes dark and declares bankruptcy shortly thereafter.
April 2014	Andrew Auernheimer is released from prison after serving only 13 months.
May 19, 2014	The United States indicts five members of the People's Liberation Army Unit 61398—the cyberattack unit of the Chinese military. This is the first time in the United States that criminal charges are filed against state actors from another country for cybercrime.
June 14, 2014	Tesla Motors releases its electric vehicle patents into the public domain.
2014	The Bitcoin exchange Mt. Gox files for bankruptcy after $460 million was apparently stolen by hackers due to "weaknesses in their system," and another $27.4 million goes missing from its bank accounts.
2014	Sony Pictures is hacked by a group called the Guardians of Peace.
2014	The computer system for the U.S. White House is hacked.
2014	The Cybersecurity Enhancement Act is passed by the U.S. Congress. The law creates a partnership between public and private agencies to increase cyber safety.
July 19, 2015	The Impact Team begins to publish sensitive information from Ashley Madison, a website that offers hookup services to members.
2015	The Ashley Madison website that encourages sexual affairs by married individuals is hacked and the names of customers are made public.
2015	Hackers gain access to the U.S. Office of Personnel Management and view the personal records of 21.5 million people, including their social security numbers, dates of birth, addresses, fingerprints, and security clearance information. The majority of the victims are employees of the U.S. government.

2015 A law called the Cybersecurity Workforce Assessment Act of 2015 is passed by the U.S. Congress. The goal of the legislation is to provide education and training to employees at the Department of Homeland Security to improve the cybersecurity. Another goal is to increase collaboration between federal agencies.

February 16, 2016 The FBI files a motion to compel Apple to assist them in bypassing the security measures on an Apple phone belonging to one of the suspects in the San Bernardino shooting.

March 28, 2016 The FBI asks that their motion to compel Apple be vacated as the FBI is able to bypass the security measures on the phone using a third party.

July 6, 2016 *Pokémon Go*—a game playable on mobile phones that has players travel to physical locations to capture virtual creatures known as Pokémon—is released in the United States. The use of GPS by the game allows some criminals to lay in wait at key physical locations and steal mobile phones from victims who visit those locations.

December 2016 The first issue of *Ledger*—the first peer-reviewed academic journal devoted to the field of cryptocurrencies—is published.

2016 Wikileaks publishes documents leaked from the Democratic National Committee.

January 17, 2017 President Barack Obama commutes the sentence of Chelsea Manning, who had been sentenced to 35 years in federal prison.

May 17, 2017 Chelsea Manning is released from custody at Fort Leavenworth, Kansas.

2017 White supremacists march in Charlottesville, Virginia. Several participants are doxed.

2017 CNN discovers the identity of a Reddit user who originally created a meme of Donald Trump beating up a person whose head had been replaced by the CNN logo. Though CNN does not publish the user's personal information, CNN appears to threaten to release such information if the user posts any offensive content in the future.

2017 The hacker group "The Dark Overlord" attempts to extort officials at entertainment company Netflix and threaten to post unreleased episodes of the Netflix show *Orange Is the New Black* online. Netflix does not give in to the demand and the episodes were posted.

May 12, 2017	The ransomware “WannaCry” is released, infecting an estimated 230,000 computers around the world.
2017	The Equifax Breach is reported. The names, addresses, birthdays, social security numbers, and other personal information of 143 million Americans are possibly stolen by cyber criminals.
2017	The Personal Data Notification and Protection Act of 2017 is passed by the U.S. Congress. It requires businesses and organizations to notify customers or clients if their personal information is hacked.
May 8, 2017	Apple removes digital rights management from its song library on iTunes.
2017	Equifax breach occurs.
2017	Deloitte breach occurs.
April 11, 2019	Julian Assange is arrested in the United Kingdom for skipping bail on an extradition hearing for rape charges out of Sweden.
May 23, 2019	The United States returns a superseding indictment on Julian Assange for his involvement, along with Chelsea Manning, in disclosing classified documents from the U.S. military regarding the wars in Iraq and Afghanistan.

A

ABANDONWARE

Abandonware is software with intellectual property rights that have supposedly been abandoned by the owner of those rights. It differs from freeware and shareware in that the intellectual property rights are not explicitly waived. In fact, with abandonware, those rights are not necessarily waived at all. Rather, those rights are simply (for the time being) not enforced by the rights holder.

A piece of software is generally deemed to be abandonware if the software is several years old, is no longer commercially available, and is no longer supported by the rights holder (Khong, 2005). However, this is not a valid assessment of the software's legal status. There is no legal recognition of abandonware. In the United States, rights holders do not lose their rights through inaction. Indeed, there are reasons why rights holders may not support a piece of software, yet would still be interested in preventing unauthorized use of their abandoned software. Rights holders may abandon a piece of software if they have developed an updated version of that software (Khong, 2005). In such an instance, the unauthorized use of the older version of the software arguably lessens the profitability of the updated version of the software because those unauthorized users are less likely to purchase the updated software. Enforcing their rights makes economic sense. Also, a rights holder may temporarily make a piece of software unavailable for strategic commercial purposes, the belief being that if a product is continuously available, the value of that product drops (Khong, 2005). Unauthorized use of the software during this period of unavailability clearly thwarts the economic goals of the rights holder, and enforcement makes sense in this instance as well.

There are instances where a rights holder may truly abandon a piece of software and have no intent to enforce those rights, such as where it is no longer economically viable to market and support a piece of software (Khong, 2005). In those instances, there may be no repercussion for someone who infringes on those rights (e.g., downloading the software without permission). However, this does not mean that the action is legal. Indeed, anyone who downloads abandonware without the permission of the rights holder runs the risk that the rights holder might ultimately decide to enforce their rights, and those who have violated those rights could face legal repercussion (Register of Copyrights, 2015, pp. 34–35).

Although unauthorized use of abandonware is not legal per se, in some instances it might be considered an orphaned work. An orphaned work is one where the rights holder is impossible to locate—not merely commercially unavailable and unsupported. Any copyrightable work—not just software—with a rights holder who is not locatable could be an orphaned work. Thus, pictures and documents can also be orphaned works—both physical copies and digital copies. Deciding how to handle orphaned works has become a pressing issue for governments in the digital age.

The European Union allows certain institutions—such as libraries, museums, or public broadcasting organizations—to reproduce and make available orphaned works if that institution conducts a thorough search and cannot locate the rights holder of a work. Canada permits citizens to apply for a conditional, nonexclusive license to use an orphaned work. This also requires the applicant to show they could not locate the rights holder after a thorough search. Japan has a system similar to Canada's, but it also requires applicants to deposit money that would ultimately go to the rights holder should they ever be located (Register of Copyrights, 2015).

Presently, the United States does not have comprehensive legislation concerning orphaned works. There is a provision of the Music Modernization Act (signed into law on October 11, 2018) that permits citizens to apply for the right to use orphaned works in limited circumstances. Specifically, use is only permitted for sound recordings made before 1972—and when prospective users of the sound recordings file notice with the copyright office that they intend to use the sound recording for noncommercial purposes. Before prospective users are legally permitted to use the sound recordings, they must wait 90 days to allow the rights holders to come forward and establish that they are the owners of the sound recordings.

The instances in which the use of orphaned works are legally permitted are severely limited. The likelihood of the use of abandonware by citizens being permitted under these laws is low. Regulations appear to be aimed at allowing the use of orphaned works for the public good (such as permitting libraries to archive the works for public search) and noncommercial use. This would, for example, certainly exclude a citizen from downloading a free copy of an old video game that is no longer commercially available or supported by the company that produced it.

See also: Copyright Infringement; Open-Source; Public Domain

Further Reading

Khong, Dennis W. K. 2005. "Orphan works, abandonware and the missing market for copyrighted goods." Paper presented at the Workshop on the Law and Economics of Intellectual Property and Information Technology, Università Carlo Cattaneo, July 22–23, 2005. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.531.5224&rep=rep1&type=pdf

Register of Copyrights. 2015. *Orphan works and mass digitization*. Washington, D.C.: United States Copyright Office.

ABENE, MARK (1972–)

Mark Abene, also known as Phiber Optik, was widely recognized as a phone hacker in the 1980s. He was one of the first hackers to defend the practice of hacking, explaining that it can be used as a constructive tool for industry. He described how hackers today can carry out much more devastating attacks than in the past, and those knowledgeable about computers can apply those skills to detecting cyberattacks before they occur.

A high school dropout, he grew up in Queens, New York, where he played on the computers in a department store while he waited for his parents to shop. At the time, computers were run through phone lines, and because the cost of the service was based on time, using them was sometimes quite expensive. Abene discovered a series of online bulletin boards through which users traded passwords and calling card numbers that allowed a user to evade the costly phone charges (a practice known as phreaking).

As he got older, Abene continued to be interested in phone phreaking and exploring the technology behind what makes a phone work. He was also motivated by the desire to learn more about the phone systems and how to defeat the security that was placed on many systems. He started to check books out at the local library to learn more about programming languages, but he found much of it to be dated. He found that he could learn more by hacking into systems himself.

Abene found he could also learn from members of a hacking group that went by the name Legion of Doom (LOD). They hacked into telecommunications systems largely to learn more about the technology. Toward the end of the 1980s LOD started to fall apart, so in the early 1990s, Abene associated himself with another hacking group called the Masters of Deception (MOD) and became a founding member.

In January 1990, law enforcement believed that Abene was behind the crash of AT&T's telephone system that left 60,000 customers without phone service for nine hours. Agents from the Secret Service raided Abene's home and seized property, but the company soon realized that the shutdown was the result of a computer software bug and not Abene. Agents again searched Abene's home in 1991, this time finding evidence of other cybercrimes. Even though Abene was a minor, he was charged with state crimes of computer tampering and computer trespassing. He accepted a plea deal to a misdemeanor crime and was sentenced to 35 hours of community service.

In December 1991, Abene again found himself in legal trouble. He and other members of MOD were indicted by a grand jury on 11 criminal counts and arrested. The prosecution presented evidence collected through wiretaps. Abene and the other members of MOD faced a potential 50 years in prison and fines of over $2 million for their offenses. Abene ended up spending 10 months in federal prison in Pennsylvania. Abene claims that his conviction was largely symbolic, especially as the sentencing judge said he was using Abene to send a message to other hackers. He was a minor at the time of the offenses and played only a small role in the crimes. He also explained that he never harmed any system he hacked. Moreover, Abene by this time had a legitimate job as a system administrator. Upon his release, a celebration called "Phiberphest '95" was held in his honor.

After being released from prison, Abene was hired in various security and IT positions for a variety of companies, including Ernst and Young, and the American

Lawyer Media. He began working as a consultant on cybersecurity issues. Abene and other former members of LOD created the security consulting firm Crossbar Security, with Abene serving as company president. He also worked with Major League Baseball to write encryption routines for their streaming service, MLBtv.

Abene has appeared in many major news and media outlets, including the *New York Times*, *Washington Post*, *Harper's*, *Time Magazine*, and CNN. His exploits were detailed in the book *Masters of Deception—The Gang That Ruled Cyberspace* (1995). He often speaks at hacker conferences and security conferences, and he also often speaks to different groups about the need for increased computer security.

See also: Legion of Doom; Masters of Deception

Further Reading

Mills, Elinor. 2009. "Q&A: Mark Abene, from 'Phiber Optik' to security guru." CNet, June 29, 2009. https://www.cnet.com/news/q-a-mark-abene-from-phiber-optik-to-security-guru/

Sandberg, Jared. 1997. "An accidental hacker shows fragility of internet security." *The Wall Street Journal*, July 10, 1997. https://www.wsj.com/articles/SB868483913917460500

Slatalla, Michelle, and Joshua Quittner. 1995. *Masters of deception: The gang that ruled cyberspace*. New York: HarperCollins.

Vanian, Jonathan. 2016. "How better technology benefits companies and hackers alike." *Fortune*, September 16, 2016. https://fortune.com/2016/09/16/technology-benefits-companies-hackers/

ADVANCED PERSISTENT THREATS

An advanced persistent threat, or APT, is a type of targeted attack on a computer system that is carefully planned and carried out. The goal of an APT is to attach malicious code to a computer system and remain there, undetected, for a long period of time. While there, the APT can allow a cybercriminal to break into the agency's network and steal information. The objective is typically not to cause harm to networks or gain money but instead to steal data or information from the victim. An effective APT can be a serious threat to companies and organizations and can cause major damage to any organization that falls victim.

There have been many highly publicized APT attacks. In 2010, the Stuxnet targeted Iran's nuclear program. This preplanned and persistent attack was intended to interrupt the nuclear program in Iran and collect information on Iranian industrial infrastructure. The attack infected Windows machines in the Natanz nuclear facility through USB keys and remained in place for many months before being detected.

Another example of an APT is Operation Aurora, an attack that targeted companies such as Google, Yahoo, Symantec, and Dow Chemical in 2009–2010. It was thought to be carried out by the Elderwood Group that is based out of Beijing, China, and has a relationship with the People's Liberation Army. The attacks began in late December 2009 and continued through January 2010. The goal of the attack was to gain access to the e-mails and other documents of executives.

In the case of Google, it was thought the attack was intended to collect names of dissidents within China. In light of the attack, Google threatened to close its offices in that country.

A third example of an APT attack was GhostNet, an attack that may have been carried out by the People's Republic of China on the networks of government offices and embassies in 103 countries. The attack was alleged to have been installed in May 2007, and it went undetected until March 2009. It is alleged that the attack allowed the offenders to switch cameras and audio systems on so they could hear critical conversations.

Offenders who carry out an APT are often individuals or teams who research the company and customize the attack to the specific system. The attack may be planned for weeks or even months to ensure that the data they seek is able to be collected. The perpetrators usually have a great deal of experience, or they may have financial backing from an outside organization. They rely on sophisticated hacking techniques to gain access to a computer system. They may even use multiple methods or techniques to breach that target. In most cases, APTs are very complex attacks that are designed to skirt any security measures that have been instituted.

The offender is often able to infiltrate a company's computer system through spearphishing, which is an e-mail sent by the offender that appears to be legitimate. It provides enough information so that the offender tricks an employee into giving enough information to allow the offender to gain access to the company's network. For example, it may trick an employee into providing a username and password. An offender may provide a link to a fake website that, when accessed by the employee, provides the offender with access. In this case, the employee will be deceived into clicking on a link or opening an attachment that seems to be legitimate. Access may also be achieved through stolen credentials or a stolen or lost laptop. In other attacks, the offender has carried out a second attack on the system at the same time, which serves to distract officials from the APT attack.

As the name suggests, an APT is a persistent attack, meaning that the incident comprises a series of attacks that are ongoing or long-term. They are not designed to allow an offender to get in and out of a company's system quickly but instead allow the offender to "persist" on the system. This way, the offender is able to steal a multitude of data, including intellectual property (trade secrets) or personal information. It can also delete data or even take over a site.

Once the offender has access to a company's computer system, he or she will be able to install malware or rewrite code that will install a back door into the network, creating a vulnerability that the company is not aware of. This permits an offender to return to the system at a later date if more or different malware is needed. The hacker may also attempt to gather usernames, passwords, and other information they have as a way to gain additional access. They may be able to gather information on other infrastructure or networks or even reprogram a system.

The final step in an APT attack is extraction, in which the offender steals the information they seek while remaining hidden from the company or official. The longer they are able to remain hidden, the longer they can continue to collect data or cause damage.

Most experts agree that it is extremely challenging for a company or organization to protect against an APT attack. There are thousands of variations of threats and attacks, so it is difficult to defend against all possibilities. Most offenders are extremely skilled, so they are able to hide their attacks from the victim. There are typically no warning signs or signals that an event is taking place, so they are difficult to detect. One suggestion to detect an APT is to look for an increase in the number of people who log onto the system at night. This is because most employees or others associated with a company do not tend to log on after business hours. Another suggestion is to install virus detection software on an organization's computer system or to use a firewall to protect it from attacks. It is also critical to train employees to not grant access to unknown people or to open attachments from unknown people. Employees should be urged to use better, more complex passwords. Other suggestions are to patch any vulnerabilities in the system as soon as they are identified and filter employee e-mails to prevent phishing attacks.

See also: Malware; Operation Aurora; Operation Olympic Games

Further Reading

FireEye. "Anatomy of advanced persistent threats." https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html

Moore, Malcolm. 2009. "China's global cyber-espionage network GhostNet penetrates 103 countries." *The Telegraph*, March 20, 2009. https://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html

Zetter, Kim. 2010. "Google hack attack was ultra sophisticated, new details show." *Wired*, January 14, 2010. https://www.wired.com/2010/01/operation-aurora/

ADVANCED RESEARCH PROJECTS AGENCY NETWORK

ARPANET, or the Advanced Research Projects Agency Network, was created by the Advanced Research Projects Network (ARPA) and quickly became the forerunner of what is today's internet. ARPANET was originally created when ARPA connected computers at four separate universities in hopes of establishing a link between phone lines and communications systems without having a central base. They sought to link machines at research institutions, specifically computers held at Cheyenne Mountain, a military complex and air force base near Colorado Springs, Colorado, to computers at the Pentagon and the Strategic Air Command over telephone lines so that they could share resources. The structure formed the basis for the modern internet.

President Dwight D. Eisenhower created the Advanced Research Projects Agency (ARPA) in 1958 after the Soviet Union's launch of the satellite *Sputnik* in 1957 and the first intercontinental ballistic missile. Many people in the United States believed that the Soviet Union would quickly surpass the United States in technology and become a threat to the nation's security. Eisenhower sought to beat the Soviet Union in the development and use of technology. He hoped that ARPA would help turn the United States into a technological superpower. As such, Eisenhower located ARPA within the U.S. Department of Defense. In the early years, ARPANET was an experimental network that allowed scientists to send information to other computers by using small packets. One key scientist in this endeavor was Joseph Carl Robnett Licklider. He was convinced that computers could help humans make better decisions and create a better world, so he was eager to make computers less focused on the military functions. Largely because of his belief in computers, ARPA funded research into the development and use of computers and graphics, along with many other developments. His successor, Robert Taylor, suggested a common system to allow for better communication between computers. This idea led to the development of ARPANET. In 1967, Taylor proposed a system to link 16 universities and research centers. To do this, they developed an idea of "packet switching." Packets are small packages of information that can be transmitted across telephone lines and then "reassembled" when they reach their location. It wasn't long before universities wanted to be involved. The University of California–Santa Barbara and the University of Utah were two of the first to enter.

Charley Kline, a student at the University of California, Los Angeles, sent the first message via ARPANET on October 29, 1969. He first attempted to send the word "login" but the system crashed after only sending the first two letters. He later tried to send the word again and succeeded. In the early years, users were discouraged from sending anything that was not related to government business. It was unacceptable to send personal messages. Messages with political or commercial messages were also discouraged.

In the mid-1970s, ARPANET was transferred to the military. By then, ARPANET had been declared "operational." The name was changed to DARPA, or the Defense Advanced Research Projects Agency. DARPA was an organization within the U.S. Department of Defense that developed technology for military use. Members of DARPA often worked alongside academics, members of industry, and other government agencies.

In 1983, the technology was widely known as the "internet" and was used by the public. The following year, in 1984, the military used the ARPANET foundation to create its own Military Network (MILNET) that could be used for unclassified communications.

See also: Department of Defense, Attacks on

Further Reading

Denning, Peter J. 1989. "The ARPANET after twenty years." *American Scientist* 77, 6 (November–December): 530–534. Reprint, Moffett Field, CA: Research Institute for Advanced Computer Science.

Kremling, Janine, and Amanda M. Sharp Parker. 2018. *Cyberspace, cybersecurity, and cybercrime*. Thousand Oaks, CA: SAGE.

Levine, Yasha. 2018. *Surveillance valley: The secret military history of the internet*. New York: Public Affairs.

Salus, Peter H. 1995. *Casting the net: From ARPANET to internet and beyond*. Reading, MA: Addison-Wesley.

ADWARE

The term "adware" is a combination of the words advertising and malware. It refers to software that displays ads (pop-up ads) on computers and mobile devices as people are using the internet. In some cases, adware is also called advertising-supported software because it automatically displays ads on computers. Others have referred to it as "malvertising."

Adware may be downloaded to a computer when the users visit certain websites, or if a person downloads a game, movie, or music. There is also a great deal of adware on social media sites like Facebook and Twitter. If a person visits a website, an ad related to that site may appear later on the person's screen. For example, if a user visits a website that sells shoes, the ads that will appear will be related to those shoes or that brand of shoes. Once the adware has been downloaded to a machine, advertising material will automatically appear on the screen.

Adware can also appear if a user downloads free software. The software is often provided at no cost because of the ads. Instead of charging the consumer who downloads the software, the creator can make money from selling the ads or making a deal to display ads for another company.

Some people consider adware to be a form of malware because these programs sometimes collect user information. It can track a person's internet behavior, including the websites a user visits, and then shows ads that may be of interest to the user. Experts point out that if the adware collects data on a user without their knowledge and tracks their usage, it can be considered to be spyware.

Most often, the ads that are shown are not wanted by the user. Most people find the ads annoying or irritating, as they continue to pop up on a screen, sometimes one right after another. It can also slow down a user's device.

Programs have been created that remove adware from a user's computer. The programs can be downloaded from the internet and should be updated frequently in order to remain effective. It is also important that a person refrain from downloading software unless the source is a known, reliable source.

There was a crackdown on adware in 2005 because of allegations of deceptive advertising. In 2007, Travelocity and AT&T's Cingular division agreed not to advertise by using adware, but within a few months, it appeared that they were once again using adware.

One man who took advantage of adware was Jeanson James Ancheta. He created a software program that was downloaded through the internet onto the computers of about 400,000 victims. He was then able to remotely send adware to the computers (now "bots") he controlled. He advertised "botz4sale" to spammers, renting a minimum of 10,000 infected computers for 4 cents each. He was paid by companies who wanted to send the adware to users. It was estimated that he earned about $60,000 in six months. Ancheta was eventually tracked down by the Federal Bureau of Investigation (FBI) and indicted on 17 federal charges related to violations of the Computer Fraud Abuse Act and the CAN-SPAM Act. He was sentenced to serve 57 months in prison, ordered to pay a fine of $60,000 and pay a $15,000 restitution to the U.S. government to pay for damage committed to their computers. Officials also seized Ancheta's property, including computer software and a BMW automobile. This was the first time that an offender in the United States was charged for spreading spyware through the use of infected computers.

See also: CAN-SPAM Act of 2003; Computer Fraud and Abuse Act of 1986; Malware

Further Reading

Battersby, Jeffrey. 2015. "When adware attacks! And how to defeat it." *Macworld Digital Edition* 32, 7 (July): 108–111.

Federal Bureau of Investigation. 2006. "The case of the 'Zombie King': Hacker sentenced for hijacking computers for profit." May 8, 2006. https://archives.fbi.gov/archives/news/stories/2006/may/botnet050806

Lemos, Robert. 2015. "Spyware infects phones, adware increases on home PCs, report finds." *Eweek*, September 16, 2015, p. 1. https://www.eweek.com/security/spyware-infects-phones-adware-increases-on-home-pcs-report-finds

Menn, Joseph. 2005. "Man is accused in dealing in 'Bots.'" *Los Angeles Times*, November 4, 2005. http://articles.latimes.com/2005/nov/04/business/fi-hacker4

Paul, Ryan. 2006. "Hacker gets jail time for botnet scheme." ARS Technical, May 9, 2006. https://arstechnica.com/uncategorized/2006/05/6789-2/

Spring, Tom. 2007. "Companies can't break ties to adware." *PCWorld*, Vol. 25, Issue 6 (June): 28.

ANONYMOUS

The group Anonymous was first established in 2003, stemming from the online message board 4chan. Today, the members describe themselves as a loosely coordinated group of hackers who come together to stand against injustice of all kinds and support free speech. The members, who are called Anons, have no formal, centralized organization, nor do they have a single leader. They have attacked governments worldwide, religious organizations, and companies. The slogan of the group is, "We do not forgive. We do not forget. We are legion. Expect us," and their logo is a man wearing a suit, with a question mark in place of the man's head.

Some members have been arrested for their hacking activities, but the identity of most members remains hidden. *Time* magazine named the group one of the 100 most influential people in the world in 2012. The group includes men and women, Democrats and Republicans, old and young, rich and poor: people from different backgrounds, races, and from all geographic areas of the world. The members prefer to remain anonymous and not identify themselves, so when they appear in public, they remain "anonymous" by wearing Guy Fawkes masks, popularized in the early 2000s by the film *V for Vendetta* (2005), based on a 1989 graphic novel of the same name.

In 2006, Anonymous carried out its first incident when members raided the "Habbo Hotel," a digital space used by teenagers to visit and "hang out." Members created their own avatars and then mingled with other user avatars while staying in the hotel. An Anon noticed that the pool area of the hotel could be easily blocked by an avatar, who would in turn block anyone from going in or out of the pool area. The Anonymous membership decided to join Habbo and then to look for avatars who had black skin, Afro hair, and wore a business suit. They then blocked the pool, doorways, and other parts of the hotel. The operators for the game shut down for a short time as they attempted to make sense of what was happening. Many Anons considered this episode to be an “epic win,” or great success.

Since, then, the members of Anonymous have a long history of being involved in controversial issues. In 2008, members attacked the Church of Scientology after a video of Tom Cruise was released on YouTube. Anonymous members believed the Church of Scientology was posting misinformation about the church and its activities. After postings on the 4chan site that called for members to “take down” the Scientology website, members quickly responded. A video was released that criticized the church and the misinformation appearing in their materials. Anonymous also protested the church’s criticism of those who dissent against Scientology or who choose to leave the organization. Anonymous members launched a distributed denial-of-service (DDoS) attack on the church that took down the website for a short time. Another time, the group ordered pizzas to be delivered to Scientology offices around the world as a way to disrupt their daily routine. In 2008, members, wearing masks, protested in front of Scientology churches. The attacks became known as “Project Chanology.”

In 2010, after the FBI shut down MegaUpload because of copyright infringement, Anonymous tackled a software company that worked with film studios and launched DDoS attacks on websites of copyright infringers. The attack on the company, Aiplex Software, shut down the website for a day. Members of Anonymous also attacked the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA), bringing down their sites. They also brought attention to various law firms, releasing data about cases handled by the firms. This was followed by an attack on Copyright Alliance, a group that works to protect copyrights and oppose internet piracy. The name given to this was Operation Payback. After these attacks, Anonymous member Christopher Whitehead (aka Nerdo) was arrested in the United Kingdom and sentenced to 18 months in prison for his role in the operations.

In November 2010, members of Anonymous launched DDoS attack and use botnets on PayPal, bringing the site down for brief periods on December 8 and 9. They did this in response to PayPal’s decision to stop taking donations in support of Julian Assange after his company, Wikileaks, released stolen top-secret documents to the public. Anonymous supported the release of the documents and saw PayPal’s decision as a form of censorship. This attack was also known as Operation Avenge Assange. In response, law enforcement arrested many Anonymous members for their hacking activities in the United States, the United Kingdom, and the Netherlands.

The following year, in 2011, the group attacked officials in the BART subway system in San Francisco after the police shot an unarmed passenger and then shut off cell phone service to thwart a protest. Anonymous members hacked into MYBART.org, the organization’s website, and posted users’ personal information. Anonymous members posted nude pictures of the company’s spokesperson online.

Members gave their support to the Arab Spring movement in 2011 in Operation Egypt. The members helped dissidents gain access to sites that had been censored by the government. They also kept websites available for those involved in the protests.

In 2011, the CEO of HBGary Federal, Aaron Barr, announced that the cybersecurity company had been able to hack into Anonymous sites and would begin to make information about the members available to the public. In response, Anonymous hacked into the HBGary website, replaced the company logo with the Anonymous logo, and then attacked the e-mail system and took down the phone system. They also hacked into Barr's Twitter account.

Anonymous members have often used their hacking skills to carry out more positive deeds. In Operation Darknet, members hacked into sites on the dark web that provide images of child pornography. The members also gained access to Hidden Wiki on the dark web and searched for sites with child pornography. Upon finding a site called Lolita City, the members hacked into it and released the names of over 1,500 alleged users who had visited the site. In 2017, a hacker affiliated with Anonymous shut down over 10,000 child pornography websites and stole personal data.

The website for the Westboro Baptist Church has also been the focus of Anonymous hackers. When church members threatened to protest the funerals of children killed in the December 14, 2012, Sandy Hook Elementary School shootings in Newtown, Connecticut, the group hacked into the church computer systems and published personal information from church members. They then were able to bring down the church's website after a DDoS attack.

After the *Charlie Hebdo* shootings in Paris, France, in January 2015, Anonymous condemned the attack and declared war on the terrorists who carried out the attacks, threatening to bring down the accounts affiliated with the terrorists. Anonymous members threated to also attack the terrorist organization the Islamic State of Iraq and Syria (ISIS) after the November 2015 terrorist attacks in Paris. Anonymous published online the Twitter accounts from almost 4,000 pro-ISIS supporters. Information on President Barack Obama and the *New York Times* was published online as well.

On August 9, 2014, police officer Darren Wilson shot and killed African-American teenager Michael Brown in Ferguson, Missouri. Following Brown's death and along with the subsequent street protests in the city, Anonymous initiated Operation Ferguson. They threatened to take down the city's servers if any protesters were harmed. In the end, Anonymous attacked the city's e-mail system, brought down the phone system, and made the internet at City Hall unavailable for a short time. In a similar attack, Anonymous also shut down the website for the city of Cleveland after two police officers shot and killed 12-year-old Tamir Rice on November 22, 2014.

The members of Anonymous continue to work for fair treatment and open government. In 2013, one of the members, Deric Lostutter, sought to expose a cover-up related to the Steubenville, Ohio, rape case in which young men from the high school football team raped a woman who was unconscious. Lostutter hacked into the website of the team's fans and found e-mails and details about team members who were part of the "rape crew." In so doing, Lostutter released and made public personal e-mails regarding the possible scandal were uncovered and made public.

In response to an antiterrorism bill passed in Canada in June 2015, Anonymous members launched a denial-of-service (DoS) attack on the servers for offices in the Canadian government. The group's members flooded the website with requests so that the site was overwhelmed and shut down.

During the 2016 presidential elections, members of Anonymous claimed to have declared war on Republican presidential candidate Donald Trump. They threatened to release his cell phone number, social security number, and other personal information. In one attack on December 11, 2016, the website for Trump Towers was shut down for over an hour. In another attack in 2016, members were protesting the "Bathroom Law" in North Carolina, a law that required people to use the bathroom associated with the gender they were assigned at birth. To some, this proposal was perceived as an anti-LGBTQ law.

In May 2017, members of Anonymous released a video in which it informed people to prepare for World War III. They blamed the growing tensions between the United States and North Korea for the increased threat. They indicated that both countries have made strategic military moves that indicate a war is close at hand.

Although most members of Anonymous choose to keep their identities a secret, a member of Anonymous was, for the first time, identified and sent to jail for his hacking in November 2009. Dmitriy Guzner, a 19-year-old American, pleaded guilty to unauthorized impairment of a protected computer. He was sentenced to a year in a federal prison. Turkish members of Anonymous were arrested in June 2011 for their involvement in DDoS attacks on government websites. In September 2011, officials arrested Chris Doyon (Commander X) for his attacks on the website of Santa Cruz County in California. While on bail, he fled to Canada. On September 12, 2012, Barrett Brown, a journalist who posted a video that threatened FBI agents, was arrested and charged with 17 offenses. Many people from outside of the United States, including the Netherlands, Australia, Turkey, and Spain, have also been arrested for cybercrimes associated with the group. Despite that, Anonymous continues to grow and thrive.

See also: Assange, Julian; Distributed Denial-of-Service Attack (DDoS); Hacker and Hacking; Hacktivism; LulzSec

Further Reading

"Anonymous' planned outing of Klan members falls flat." 2016. *Intelligence Report*, 160 (Spring): 3–4.

Clayton, Mark. 2011. "Hacker arrests: Why anonymous might not be so anonymous." *Christian Science Monitor*, July 21, 2011. https://www.csmonitor.com/USA/2011/0721/Hacker-arrests-Why-Anonymous-might-not-be-so-anonymous

Coleman, Gabriella. 2014. *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. London: Verso.

Hunn, David. 2014. "Not-so anonymous: How hackers wreaked havoc in St. Louis." *St. Louis Post-Dispatch*, November 1, 2014. https://www.stltoday.com/news/local/crime-and-courts/not-so-anonymous-how-hackers-wreaked-havoc-in-st-louis/article_809a5d53-7d67-57ff-96f9-ee5772b395d0.html

Olson, Parmy. 2012. *We are anonymous*. New York: Little, Brown and Company.

ASHLEY MADISON BREACH

Ashley Madison is a website that assists users who seek to arrange extramarital affairs with other users. In July 2015, a group called "The Impact Team" hacked the website, threatening to make public the private information of many members if the website was not removed. When the website remained active, the group revealed members' identification, including their real names, addresses, transaction records, and sexual preferences. The group released information associated with a seven-year span, causing great embarrassment for many users. At the time, the website had about 32 million users. In addition, the information about the website's parent company's financial information and salary information was also made public.

The parent company of Ashley Madison, Avid Life Media, had a policy of not deleting the personal information of its members for the Ashley Madison site or another similar site, Established Men. When the threat to expose the membership was first made, the company claimed that they had secured their sites so that no names could be released. When the hackers released that information, the company decided to cooperate with law enforcement to investigate the attack. They offered $500,000 (Canadian, or $378,000 U.S.) for information that would lead to the arrest of the person/people behind the breach.

The hackers reportedly chose Ashley Madison because they disagreed with the site's goal of arranging extramarital affairs between married individuals. They also were upset by Avid Life's business practices, specifically the requirement that people were asked to pay a $19 fee to have their private data deleted if they changed their mind about having an affair. In many cases, even though the member paid the fee to remove their data, it remained active. The hackers claim that Avid Life made $1.7 million each year from clients who sought to delete their information.

At first, the hackers posted the information on the dark web but then listed it on the open web, where they turned it into a searchable document. Websites were created that anyone could use to investigate whether their spouses or friends had paid for a membership on the site. There was also a map created to show where the users lived. Many of the users were linked to governments in Canada and the United States, including the military. Under the Code of Military Justice, adultery is an offense that can lead to imprisonment and a dishonorable discharge. For some users for countries such as Afghanistan, Iran, and Saudi Arabia, a homosexual affair is punishable by death. About 86 percent of the users were men. Some of the members used fake names and e-mails, whereas others used the name of a real person, maybe setting up a fake account as a prank. Many of the users were blackmailed, receiving threats that messages would be sent to family and friends if they did not send money (typically in Bitcoins) to keep it quiet.

Several well-known figures were caught up in the breach, including conservative activist and television reality personality Josh Duggar of *19 Kids and Counting* (2008–2015). Dr. Walker Palmer, who made headlines in July 2015 for killing "Cecil the Lion" in Hwange National Park, in Zimbabwe, was also identified among the site's users. Joshua Cline, former aide to Michigan Republican State Representatives Todd Courser and Cindy Gamrat, was also outed as a user on Ashley Madison. Earlier that year, Cline blew the whistle on Courser and Gamrat's extramarital affair. Courser resigned his seat in September 2015, and the Michigan House of Representatives expelled Gamrat that same month.

On August 21, 2015, two law firms in Canada filed a $578 million class-action lawsuit against Avid Dating Life Inc. and Avid Life Media Inc., representing Canadian citizens who were members of Ashley Madison. The members claimed the company did not protect the users' privacy, as required under Canadian law. They were particularly upset that they paid the fees to have their personal information deleted, which did not happen. The company pointed to a statement on the website that claims that the service is a "100% discrete service." But it also states, "We cannot ensure the security or privacy of information through the Internet."

The release of the information from the website was linked to two suicides, one of whom was a priest from Louisiana. Avid Life Media chief executive officer Noel Biderman resigned on August 28, 2015. The original company, Avid Life, was rebranded as Ruby. It was found that Ruby created false profiles of women on the site as a way to lure men into joining.

U.S. law enforcement, the U.S. Federal Trade Commission (FTC), and officials in Canada and Australia investigated the hacking. The company was found guilty of lax security and deceptive practices. In December 2016, the U.S. FTC fined the company $24 million. However, because of their inability to pay the full amount, the company only paid a fine of $1.66 million. The customers whose data was made public did not receive any financial payment, but many have joined in class-action lawsuits against the company.

The website is still available. Since September 2015, the company claims to be willing to fully delete people's data if they choose. The company claimed that it has updated its security.

See also: Hacker and Hacking

Further Reading

Marking, Havana, and Marc Morgenstern. 2016. *Ashley Madison: Sex, Lies and Cyber Attacks*. Documentary film.

Middleton, Bruce. 2017. *A history of cyber security attacks: 1980 to present*. Boca Raton, FL: CRC Press.

Ottomano, Jason P. 2017. "What would grandma say? How to respond when cyber hackers reveal private information to the public." *Cornell Law Review* 102, 6 (September): 1743–1765.

Robinson, Teri. 2015. "Extramarital website Ashley Madison hacked." *SC Magazine: For IT Security Professionals*, July 20, 2015. https://www.scmagazine.com/home/security-news/extramarital-website-ashley-madison-hacked/

ASSANGE, JULIAN (1971–)

Julian Assange is the founder of WikiLeaks, an organization dedicated to organizational transparency through the release of confidential and other sensitive documents. As of 2019, Assange officially faces criminal charges in the United States for his role in disclosing confidential documents provided to him by Chelsea Manning in 2010 regarding the U.S. wars in Iraq and Afghanistan. He was arrested in London in 2019 and faces extradition to the United States to face those criminal charges.

Assange was born in Townsville, Australia, on July 3, 1971. Growing up, Assange did not receive a formal education. He at times took correspondence courses, was home-schooled, and studied informally with university professors. During this time, his mother bought him his first computer, and he learned how to program, and how to hack (Khatchadourian, 2010; Kwek, 2010). Assange adopted the hacker moniker Mendax and helped form a hacker group known as the International Subversives. While working with the International Subversives, Assange hacked into the computer systems of Nortel—a Canadian telecommunications company—that were located in Melbourne, Australia. Police approached Assange about the hack on October 29, 1991, and he was charged with 31 counts of hacking shortly thereafter (Khatchadourian, 2010). The case was ultimately resolved in 1995. Assange pled guilty to 25 of the 31 counts against him. The judge did not require Assange to serve any time in prison as part of the sentence (Kwek, 2010).

In 2006, Assange founded WikiLeaks, an organization that releases confidential and similar material that it feels the public should know about. This has included leaks of government material—such as documents pertaining to Guantanamo Bay in 2011—and leaks of material from private organizations—such as the secret bibles of Scientology in 2008. The leak that is perhaps most well-known is the 2010 leak of United States military documents regarding military operations of the United States in Iraq and Afghanistan. Notable among those documents is footage of U.S. military helicopters killing several people—among whom were journalists—dubbed "Collateral Murder" (WikiLeaks, 2010). These disclosures attracted the attention of the United States government. Shortly after these leaks were made, Attorney General Eric Holder stated there was an active investigation of Assange and WikiLeaks (Weiss, 2010). It was later revealed in 2018—albeit inadvertently—that Assange had in fact been charged with crimes in the United States, though the exact crimes he has been charged with is still unknown (Zapotosky and Barrett, 2018). An indictment that superseded the prior indictment against Assange was made public in 2019, following his arrest. Assange was charged with 18 counts stemming from his disclosure of the documents provided to him by Chelsea Manning—an army intelligence officer. The charges allege that Assange conspired with Manning to obtain the documents and disclose them, with Assange at one point agreeing to crack a government password for Manning in order to gain access to information Assange and Manning were seeking (United States Department of Justice, 2019).

Assange has also faced legal issues outside of his activities with WikiLeaks. In 2010, Assange is alleged to have committed rape in Sweden, and he was charged accordingly. Swedish authorities issued a warrant for his arrest. Assange and his legal team believe the charges were politically motivated based on Assange's involvement with WikiLeaks (Davies, 2010). Assange initially submitted to the warrant in the United Kingdom on December 8, 2010. He was released on bail eight days later on December 16. On August 16, 2012, Assange was granted asylum by Ecuador, and he took up residence at the Ecuadoran embassy in London. Assange had been staying in the embassy prior to that and skipped bail during that time. He had been living there since that time up until his arrest in 2019 (BBC News, 2018). Swedish authorities dropped the arrest warrant for Assange in 2017. Assange's legal team has claimed this to be a victory for their client, though it appears the dismissal was due to procedural reasons, not factual ones. The inability of Swedish authorities to serve Assange with the necessary legal paperwork while he was in the Ecuadoran embassy appears to have necessitated the dismissal (see BBC News, 2017). Despite the Swedish warrant being dismissed, the judge on Assange's case in the United Kingdom refused to dismiss charges against him for skipping bail (Khomami, 2018). Following Assange's arrest, he was sentenced to 50 weeks in prison for skipping bail (Sharman, 2019). Sweden also decided to resume its investigation into rape charges against Assange and announced it would seek extradition of Assange again (Chappell, 2019). The United States, based on the indictment mentioned above, already has an extradition request in place with the United Kingdom. Assange's legal team believes it would be impossible for him to receive a fair trial in the United States (Chappell, 2019). This may stem in part from the political nature of the crimes he is alleged to have committed. Seeing the sentence that Manning (his alleged coconspirator) received—35 years in prison—may also play some part in his legal team's assessment.

Assange was arrested by law enforcement in the United Kingdom on April 11, 2019. It appears that he may have overstayed his welcome in the Ecuadorian embassy, leading to his expulsion from the embassy and his ultimate arrest. During Assange's residency at the Ecuadorian embassy, there were occasional indications that Ecuador was growing frustrated with him. In March 2018, Ecuador cut off Assange's telephone and internet access. It also prohibited in-person visitation with others, except for his legal team (Meek and Dukakis, 2018). These privileges were partially restored in October 2018 (Greenfield, 2018). Ecuador indicated that the reason for the restriction was Assange's violation of "a written commitment made to the government at the end of 2017 not to issue messages that might interfere with other states" (Greenfield, 2018; Meek and Dukakis, 2018). Following Assange's arrest, Ecuador claimed that he had been a problematic guest, stating that he had mistreated staff at the embassy, failed to properly take care of his pet cat, and was generally messy—Ecuador claimed he at one point spread fecal matter on the walls. Assange's legal team disputes these allegations. These actions, however, do not appear to be the basis for Assange's eviction. Ecuadoran President Lenin Moreno stated the reason for Assange's eviction was the actions Assange took against foreign governments while housed at the embassy. Said Moreno, "We cannot allow our house, the house that opened its doors, to become a center for spying" (CBS News, 2019).

Indeed, despite being confined in the Ecuadorian embassy in London since 2012, Assange has remained involved in the affairs of WikiLeaks. One notable example is his involvement in WikiLeaks's publishing of numerous e-mails of the Democratic National Committee during the 2016 U.S. presidential election. There have been claims that the e-mails originated from Russia. Assange has denied that Russia was the source of the e-mails but—in following with WikiLeaks's practice—has not disclosed who the source was. Assange also offered assistance to Edward Snowden, a National Security Agency (NSA) contractor who leaked numerous NSA documents in 2013. Though Snowden did not leak the NSA documents through WikiLeaks, Assange made arrangements for Snowden to also seek Ecuadorean asylum. While Snowden's passage to Ecuador was ultimately blocked, he was able to make it to Russia with the assistance of Assange's associate Sarah Harrison (Burrough and Ellison, 2014).

See also: Hacker and Hacking; Manning, Chelsea; Snowden, Edward; WikiLeaks

Further Reading

BBC News. 2017. "Julian Assange: Sweden drops rape investigation." *BBC News*, May 19, 2017. https://www.bbc.com/news/world-europe-39973864

BBC News. 2018. "Julian Assange in the Ecuadorian embassy: Timeline." *BBC News*, October 19, 2018. https://www.bbc.com/news/world-europe-11949341

Burrough, Bryan and Sarah Ellison. 2014. "The Snowden saga: A shadowland of secrets and light." *Vanity Fair*, May 2014. https://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview

CBS News. 2019. "Ecuador's leader says Julian Assange turned London embassy into a 'center of spying.'" *CBS News*, April 15, 2019. https://www.cbsnews.com/news/julian-assange-wikileaks-ecuador-embassy-center-spying-lenin-moreno-04-15-2019/

Chappell, Bill. 2019. "Sweden reopens inquiry into Julian Assange over rape allegations." *NPR*, May 13, 2019. https://www.npr.org/2019/05/13/722765304/sweden-reopens-inquiry-into-assange-over-rape-allegations

Davies, Nick. 2010. "10 days in Sweden: The full allegations against Julian Assange." *The Guardian*, December 17, 2010. https://www.theguardian.com/media/2010/dec/17/julian-assange-sweden

Greenfield, Patrick. 2018. "Julian Assange to regain internet access at embassy base—Reports." *The Guardian*, October 14, 2018. https://www.theguardian.com/media/2018/oct/14/julian-assange-to-regain-internet-access-in-embassy-base

Khatchadourian, Raffi. 2010. "No secrets: Julian Assange's mission for total transparency." *The New Yorker* 86, 16: 40.

Khomami, Nadia. 2018. "Judge refuses to withdraw Julian Assange arrest warrant." *The Guardian*, February 13, 2018. https://www.theguardian.com/media/2018/feb/13/judge-refuses-to-withdraw-julian-assange-arrest-warrant

Kwek, Glenda. 2010. "Magnet for trouble: How Assange went from simple island life to high-tech public enemy number one." *The Sydney Morning Herald*, December 8, 2010. https://www.smh.com.au/technology/magnet-for-trouble-how-assange-went-from-simple-island-life-to-hightech-public-enemy-number-one-20101208-18pb3.html

Meek, James Gordon and Ali Dukakis. 2018. "Assange in 'solitary confinement' at embassy, fears possible extradition to US, lawyer says." *ABC News*, August 3, 2018. https://abcnews

.go.com/Politics/assange-solitary-confinement-embassy-fears-extradition-us-lawyer/story?id=57018760

Sharman, Jon. 2019. "Julian Assange: Wikileaks founder drops appeal against prison term for breaching bail." *Independent*, July 18, 2019. https://www.independent.co.uk/news/uk/crime/julian-assange-prison-appeal-breach-bail-belmarsh-sweden-wikileaks-a9011131.html

United States Department of Justice. 2019. "WikiLeaks Founder Julian Assange charged in 18-count superseding indictment." United States Department of Justice, May 23, 2019. https://www.justice.gov/opa/pr/wikileaks-founder-julian-assange-charged-18-count-superseding-indictment

Weiss, Baruch. 2010. "Why prosecuting WikiLeaks' Julian Assange won't be easy." *The Washington Post*, December 5, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/12/03/AR2010120303267.html

WikiLeaks. 2010. "Collateral murder." *WikiLeaks*. https://collateralmurder.wikileaks.org/en/index.html

Zapotosky, Matt and Devlin Barrett. 2018. "Julian Assange has been charged, prosecutors reveal inadvertently in court filing." *The Washington Post*, November 15, 2018. https://www.washingtonpost.com/world/national-security/julian-assange-has-been-charged-prosecutors-reveal-in-inadvertent-court-filing/2018/11/15/9902e6ba-98bd-48df-b447-3e2a4638f05a_story.html?utm_term=.ef8637965bc8

AUERNHEIMER, ANDREW ALAN ESCHER (1985–)

Andrew Auernheimer, also known as Weev, is known for being a black-hat hacker and internet troll, a behavior he carries out to "(see) people suffer ironic punishments" (Kunzelman, 2017). Auernheimer has also been associated with a hacking group known for attacking universities and has become recognized for using racist and anti-Semitic rhetoric. In 2009, he participated in an attack on Amazon in which books on LGBTQ issues were reclassified as pornography.

In 2010, Auernheimer was part of a group called Goatse Security that hacked into the computer systems of AT&T. He then uploaded the e-mail addresses of 114,000 iPad users that included the addresses of well-known celebrities, including Michael Bloomberg, the mayor of New York; Diane Sawyer, a journalist with ABC News; Rahm Emanuel, the former White House Chief of Staff and mayor of Chicago from 2011 to 2019; and many military members, including Colonel William Eldredge from the Air force. Other passwords were those that belonged to employees of National Aeronautics and Space Administration (NASA), the Defense Department, the Justice Department, and the U.S. Department of Homeland Security (DHS).

In explaining his actions, Auernheimer said that companies should do the right thing and let people know if there is a security problem with the company (Worthen and Spencer, 2010). He said that he was able to access the company's information with little skill because the security was so lax. He gave AT&T's data to the press as a way to inform customers of the negligence with which the company treats personal data (Rensin, 2014). He sought to publicize flaws in companies so they will be encouraged to fix them and keep people's data secure. He claimed that he hacked into the company's site as a way to help AT&T increase its security.

In 2010, Auernheimer was investigated and arrested on drug charges. He was charged with possession of cocaine, LSD, and ecstasy. During the process, he criticized the search of his home. The charges were dropped in January 2011. But at that time, he was arrested and charged with one count of conspiracy to access a computer without authorization and one count of fraud. Because he did not have a job, Auernheimer was denied bail. He was transferred to the Federal Center in Oklahoma and released on $50,000 bail in February 2011.

In July of 2011, Auernheimer was indicted on one count of conspiracy to gain unauthorized access to computers and one count of identity theft. He was found guilty of these charges in November 2012 and then sentenced to spend 41 months in federal prison, with an additional three years of supervised release. He was also ordered to pay $73,000 in restitution to AT&T. He was sent to a low-security federal correctional institution in Allenwood, Pennsylvania, where he spent time in solitary but also participated in a hunger strike.

Auernheimer appealed his conviction, and in April 2014, the Third Circuit Appeals Court decided to overrule the conviction based on the fact that the venue was improper. He was charged in New Jersey but his crimes occurred in Arkansas. Auernheimer was released from prison in April 2014 after serving only 13 months. Upon his release, he asked that the government compensate him for the time he spent in prison. He demanded 28,296 Bitcoins (about $13.2 million), which was one Bitcoin for each hour he served. He refused to accept U.S. currency because it is the preferred currency of "criminal organizations" including the FBI, the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), and the Federal Reserve (Musil, 2014).

Auernheimer serves as the webmaster for *The Daily Stormer*, a neo-Nazi journal that appears on the dark web because Google refuses to host the site. In that journal, he wrote that he was treated harshly because the judge in his case was African-American. He also ranted about the evilness of Jews and left a lewd message on the answering machine of a Jewish woman in Montana. In an article in October, 2014, Auernheimer described himself as a white nationalist. Moreover, Auernheimer is banned from Twitter because of the racial tone of his tweets in that media.

In 2014, Auernheimer moved to Lebanon to avoid any further punishment from the U.S. government. In October 2015, he was working to publish the names of the government employees whose names appeared on client lists of the Ashely Madison website, a site that endorses extramarital affairs.

In 2016, Auernheimer programmed thousands of printers at universities to print thousands of anti-Semitic flyers with swastikas, addressed to "white men." Under the Junk Fax Prevention Act of 2005, it is illegal for people to send unsolicited ads to a fax machine without an established business relationship with the recipient, and the recipient must have provide their fax number to the sender voluntarily. He could be fined $500 per flier.

See also: Ashley Madison Breach; Black-Hat Hackers; Cyberbullying; Dark Web; Hacker and Hacking

Further Reading

Gutman, Rachel. 2018. "Who is Weev, and why did he derail a journalist's career?" *The Atlantic*, February 14, 2018. https://www.theatlantic.com/technology/archive/2018/02/who-is-weev/553295/

Hayden, Michael Edison. 2018. "Neo-Nazi who calls for 'slaughter' of Jewish children is of Jewish descent, his mom says." *Newsweek*, January 3, 2018. https://www.newsweek.com/neo-nazi-andrew-weev-auernheimer-daily-stormer-jewish-descent-768805

Kunzelman, Michael. 2017. "Notorious troll calls the online tactics 'a national sport.'" AP News, March 29, 2017. http://apnews.com/04c73bb948ce4182845a6d27e0a9c3e1.

Musil, Steven. 2014. "AT&T hacker 'Weev' sends feds 'invoice' for time in prison." cnet, May 20, 2014. https://www.cnet.com/news/at-t-hacker-weev-sends-bitcoin-invoice-to-feds-for-time-in-prison/

Rensin, Emmett. 2014. "This infamous hacker went to prison for trolling AT&T. Now he wants to troll Wall Street." *New Republic*, April 22, 2014. https://newrepublic.com/article/117477/andrew-weev-auernheimers-tro-llc-could-send-him-back-prison

Worthen, Ben, and E. Ante Spencer. 2010. "Computer experts face backlash." *Wall Street Journal*, June 14, 2010. https://www.wsj.com/articles/SB10001424052748703885104575303032919382858

AWARENESS

Cybercrime awareness refers to not only to one's knowledge of what cybercrime is but also to one's knowledge of how cybercrimes are carried out. As cybercriminals are always evolving in the ways they commit cybercrime, so too must individuals be on top of these evolutions to be truly aware of cybercrime and the risks it poses.

Helping everyone become aware of cybercrime is important for government and businesses. While a business or government agency can employ individuals whose specific job is cybersecurity, none of that matters if individual employees compromise confidential information because they are unaware of the methods being used against them. Accordingly, businesses and governments may take steps to make their employees (and others) aware of cybercrime risks.

In the United States, the DHS includes tips for protection against cybercrime on its website (Department of Homeland Security, 2018). These tips include choosing a password that will not be easily guessed, keeping software on a computer and other devices updated, and securing Wi-Fi networks. Tips are even provided for handling emerging technologies. For example, smart home technology is becoming more popular, allowing people to access door locks, security cameras, garage doors, lights, and other aspects of their home via cellphone. If cybercriminals are able to hack into the smart home application a homeowner is using, they could gain entrance into that home.

The DHS recommends several tips for individuals using smart home technology, including regularly reviewing the mobile applications used (including ones to run a smart home) and deleting those that cannot be verified as reputable and those the owner does not regularly use. DHS also suggests disabling features on cell phones that geo-tag (i.e., let others know the phone's current location using GPS technology to find and broadcast that location). People may use this feature to let friends and family know where they are, but if a cybercriminal were to gain access to that information in conjunction with hacking into a smart home account, not only could the cybercriminal break into that person's house, but they would know the best time to do it based on the homeowner's location.

While not necessarily a crime in every state, cyberbullying is often included in the general discussion of cybercrime awareness. The dangers posed by cyberbullying differ from those posed by cybercrime in general. Much of the danger posed by cybercrime is financial loss. While there are hundreds of thousands of individuals who fall victim to cybercrimes each year (see Federal Bureau of Investigation, 2018), businesses are regularly and repeatedly attacked by cybercriminals. It is estimated that the average American business is attacked 4 million times per year, with businesses specifically involved in financial services being attacked 1 billion times per year (Mirchandani, 2018). The danger posed by cyberbullying is not so much financial loss as it is psychological harm. The predominant targets of cyberbullying differ from cybercrime in general as well. It appears that minors, in particular, tend to be the victims of cyberbullying. It was estimated in 2013 that just under 7 percent of people between the ages of 12 and 18 had been cyberbullied at some point (United States Department of Education, 2015). The United States government provides tips for parents to protect their children against cyberbullying (see Stopbullying.gov., 2019). Recommendations include monitoring children's internet activity and establishing rules governing children's internet usage.

In attempts to regularly raise awareness of cybercrime, both the United States and the European Union have designated October as Cybercrime Awareness Month. Additionally, Safer Internet Day is celebrated in over 140 countries—including the United States, the United Kingdom, China, and Russia. It was first celebrated on February 6, 2004, and is currently celebrated on the Tuesday of the second week in February (the second day of the second week in the second month). The purpose of Safer Internet Day is to increase awareness of safety concerns that exist on the internet, including cyberbullying and other cybercrimes.

See also: Cyberbullying; Password; Vulnerability

Further Reading

Department of Homeland Security. 2018. "National Cybersecurity Awareness Month resources." https://www.dhs.gov/publication/national-cyber-security-awareness-month-resources

Federal Bureau of Investigation. 2018. *2017 internet crime report*. Washington, D.C.: Federal Bureau of Investigation.

Mirchandani, Bhakti. 2018, August 28. "Laughing all the way to the bank: Cybercriminals targeting U.S. financial institutions." *Forbes*. https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#49fc213a6e90

Stopbullying.gov. 2019. "Digital awareness for parents." Stopbullying.gov. https://www.stopbullying.gov/cyberbullying/digital-awareness-for-parents/index.html

United States Department of Education. 2015. *Student reports of bullying and cyber-bullying: Results from the 2013 School Crime Supplement to the National Crime Victimization Survey*. Washington, D.C.: United States Department of Education.

B

BACKDOOR

A backdoor (sometimes called a trapdoor) is a method that hackers use to bypass security in a product or system and allow them to access files or computer networks, usually without detection. They use the backdoor to gain access to sensitive data or to achieve control of the network. Offenders can also use a backdoor to get into a system to install malware or modify code, or to install ransomware. They can send junk e-mail, or spam, from that computer. Backdoors are often used to launch a cyberattack on a company or organization. They are a way for intruders to surreptitiously access a computer system by taking advantage of a security vulnerability. Viruses and Trojan programs can install backdoors on computer systems that remain active for extended periods.

Sometimes the backdoors are widely known and publicly available, but the majority of times they are secret. In some cases, the programmer who developed the program or network administrators wrote the backdoor so that they could use it for troubleshooting in the future. However, this can pose a serious danger if the information is stolen, or if the administrator later seeks to inflict harm on the company.

Some backdoors have been designed so that a detection program will not uncover them, which makes finding the backdoor much harder. Companies should be sure to install firewalls that will block access from unauthorized users. They should also monitor their networks to uncover any unusual or suspicious behavior. Anti-malware software can also help to unearth any malware that may have been installed through the backdoor.

OceanLotus, a hacking group based in Vietnam, created and used a backdoor to launch targeted APT (advanced persistent threat) attacks on these groups. The backdoor was sent to the agencies via a Word document sent through an e-mail that appeared to be a registration form for an event sponsored by a rights organization (Horeisi, 2018).

See also: Advanced Persistent Threats; Hacker and Hacking; Malware

Further Reading

Caravut, Sinchai. 2008. *Multiple logs analysis for detecting zero-day backdoor Trojans*. Cleveland, OH: Cleveland State University Press.

Horeisi, Jaromir. 2018. "New MacOS backdoor linked to OceanLotus found." Trend Micro, April 4, 2018. https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-backdoor-linked-to-oceanlotus-found/

Trend Micro. 2015. "Backdoor attacks: How they work and how to protect against them." January 7, 2015. https://blog.trendmicro.com/backdoor-attacks-work-protect/

BANKING ATTACKS

Online banking has become the norm around the globe. Customers of all sorts, both individuals and organizations, are able to access their accounts and financial information through computers and other devices. At the same time, mobile banking means that sensitive, personal data may be stored on devices that are easily lost or hacked (Cybersecurity, 2016). Online banking give criminals more opportunities to commit theft, fraud, and other offenses. Many banks are finding it difficult to keep up with offenders as they constantly come up with new ways the use computers to commit banking-related crimes. Bank officials are often unaware they have been attacked until it is too late and significant damage has been done.

Attacks on financial institutions (banks and credit unions) have increased, and the losses have become larger, sometimes resulting in significant harms to customers. The results of a global survey of more than 60 financial institutions around the world, completed in July 2016, indicated that over 66 percent of the institutions reported that they were the victim of at least one cyberattack in the previous year. Another survey carried out by SecurityScorecard in the Spring of 2016 found that 10 percent of international companies that had been the victim of a cyberattack between June 2015 and April 2016 were financial institutions (SecurityScorecard, 2016). They also discovered that of the top 20 U.S. commercial banks, 19 received a Network Security score of C or lower. Moreover, malware was found in 15 out of the 20 banks, some of which was serious (SecurityScorecard, 2016).

Types of Attacks

A cyberattack on a bank can be devastating to the institution. It can leave the bank paralyzed, unable to operate for a period of time. Money can be stolen, or customer data can be stolen. It has been estimated that a cybercrime may cost an agency $100,000 an hour or even more (Crosman, 2015). An attack on a bank could also ruin the bank's reputation.

Banks are attractive targets for cyber-criminals due to the large amounts of cash that can be obtained from them, as well as valuable personal information from bank customers. This can include passwords, bank account numbers, and personal information. Banks can also be attractive targets for foreign governments who seek both financial rewards and private information on key clients (Cybersecurity, 2016).

There are many different types of attacks that can be used against banks. Some offenders have used DDoS attacks in which many requests for information are sent to a website simultaneously, forcing the website to shut down for a period of time. The sites can sometimes be frozen for hours. During this time, the bank is unable to help customers. There have also been extortion attacks through which banks are forced to pay money (or Bitcoin) to prevent their sites from being shut down or to protect customer data from being stolen. An offender may launch a DDoS attack or other attack on the bank as a way to disguise other financial fraud or activity that may be occurring. Sometimes, cybercriminals are able to change data during a hacking attack, make the existing data invalid (Cybersecurity, 2016).

ATM fraud, which focuses on the bank's automated teller machines, occurs when offenders create "dummy" ATM machines. When an unsuspecting customer uses the machine, it records the customer's card number and personal information number (PIN) but won't let the customer complete the transaction because it is "out of order." The stolen information is used to create a fake bank card, which is then used at a legitimate ATM or is used to purchase goods. Other offenders can steal ATM information by using cleverly placed cameras or card swipe readers.

With cyber-banking, criminals can empty an existing bank account in no time if they have the victim's account information. Criminals may use techniques to get banking information by going to the victim themselves as opposed to launching an attack on the bank. Criminals may attempt to obtain a customer's PIN or password through a phishing or spear-fishing attack, or through a virus that traces a keylogger. Offenders have also been able to convince people to give out personal information via social engineering. Once the criminal has the victim's card information and PIN, he or she can then steal money from an account. Criminals also obtain personal information by spoofing, where hackers can enter the banks' website and steal login information and passwords, or they can place a zoom lens video camera within close range to an ATM, enabling them to capture PINs. They can also use false URLs that appear to be the bank's legitimate site where customers will attempt to login, unknowingly supplying their account information to criminals.

Once they steal a victim's personal information, offenders can open bank accounts in the victim's name. This is usually done to carry out a long-term scam, get a bank loan, or get government benefits. The offender can have checks deposited into a fake account or use the name of a recipient who has died to steal social security checks or redirect automatic deposits; to get a bank loan, a person must have a bank account, so they use stolen or forged documents that are required for the loan.

In some cases, the hackers who obtain access to people's accounts are not cyber criminals but rather employees of the bank. These insiders know the system and know ways to commit fraud. They can be exploited by criminals or bribed to give out personal information.

A common type of cyberattack that banks experience is a "salami attack." This occurs when a cybercriminal steals a small amount of money from many different accounts and then puts the money into one account (so-called because of the similarities to the process of making salami). In short, a cybercriminal is said to use a salami attack when he or she removes a minimal amount of money from a fund and puts it into one larger fund. The amount is so small that the owner of the account does not detect the loss, but when this is done multiple times or over a long period of time, it can be a substantial loss to the victim. This kind of attack is often carried out against a bank or other financial institution.

In some cases, instead of money being siphoned off the top, the amounts of interest are rounded down and the money is then put into another account. Or a criminal takes a few pennies in each pay period. When this is carried out on hundreds of employees or for an extended time, the offender's account can become quite large. The victim may not be aware of the money being taken or the information being gathered. The offender is able to continue to steal money or gather knowledge sometimes for a lengthy period of time before it stops.

Attack Examples

There are many examples of cyberattacks on banks and other financial institutions. One occurred in September 2012, in retaliation for a YouTube film that some felt was offensive to Islam. A group named Izz ad-Din al-Qassam Cyber Fighters used DDoS attacks to freeze the websites of multiple financial companies such as the Bank of America, JP Morgan Chase, PNC, and Wells Fargo. The attacks were some of the largest DDoS attacks in the industry. The actual intent of the protesters was to eliminate the online presence of the different institutions as opposed to stealing funds.

Another attack in 2015–2016 resulted in the theft of an estimated $81 million dollars from banking institutions in the SWIFT banking network around the world, including Bangladesh, Vietnam, New York, and Ecuador. The attacks were carried out by a hacking group called APT 38, which is thought to be connected to North Korea. The attackers looked for vulnerabilities in the networks of banks that they then used to have access to the bank's credentials. A message was sent to other banks asking to transfer funds. It is estimated that millions of dollars were stolen from accounts. This is thought to be the first time a state actor was responsible for an attack on a financial institution.

The Carberp Trojan, a form of malware designed to steal personal information from victims, also appeared in 2013–2015. By using this malware, offenders were able to steal personal information and funds from customers. It was estimated that offenders stole a billion dollars (or more) from victims.

The victims of a different incident in 2016 included five Russian banks that suffered DDoS attacks over a two-day period. One of the bank sites received 660,000 requests for information per second, which quickly overloaded its systems (Khandelwal, 2016).

The hacking group Anonymous launched a DDoS attack on banks around the world in May 2016 in an event named Operation Icarus. On May 4, members warned banks such as the U.S. Federal Reserve, the Bank of England, the IMF, and the World Bank that "one of the most massive attacks ever seen in the history of Anonymous" was going to be launched. Their intent was not to steal money but rather to "not let the banks win." The attack shut down the bank websites for about a day (Ashok, 2016).

Member institutions in the Lloyds Banking Group experienced DDoS attacks on their accounts for 48 hours in 2017. The criminals demanded a large ransom to be paid in Bitcoin in order to stop the attack. In the end no accounts were actually attacked, and Lloyds did not pay the ransom.

Banking Security

Those who work in the banking industry must always be on the lookout for cybercriminals who seek to infiltrate their networks. Banks have increasingly become more aware of the dangers of cybersecurity and the need for countermeasures to combat it. Banks are increasing their security and are detecting attacks much earlier than in years past, often hiring better IT employees who understand risks. It seems that banks tend to respond more quickly to attacks when compared to other organizations. One survey showed that 88 percent of banks detected a cyberattack in under two hours (as compared to 77 percent of other companies); 72 percent of banks are able to respond to an attack in under two hours (as compared to 68 percent of other companies) (Crosman, 2015).

Banks need to take preventive measures to protect their customers and their organizations. Most banks have installed cybersecurity measures—but to varying degrees. It is difficult and expensive to maintain a secure system. They must be continually changing to address changing threats. Smaller agencies do not have plans in place as do larger ones. Banks need to know if there are any vulnerabilities in their systems. They need to install and continually updates malware protection. They can also increase the use of encrypted data if it is sent from one place to another. Some financial institutions do not effectively encrypt their financial data (Cybersecurity, 2016).

Preventive measures should also be taken by the customer. Individuals need to be careful not to respond to e-mails that requests bank account information or passwords. If an e-mail is questionable, the individual should call the bank (not using the contact provided in the e-mail) to ensure it is legitimate. People should also be wary of giving out their information over the phone if they receive a call purporting to be from a bank. If a person calls and appears to be a member of the staff from a bank, it may not be real. Customers should also be encouraged to change their password often, and use secure passwords.

See also: Anonymous; Carberp; Distributed Denial-of-Service Attack (DDoS); Hacker and Hacking; North Korea; Phishing

Further Reading

Ashok, India. 2016. "Op Icarus: Anonymous launches DDoS attacks on international banks." *International Business Times*. https://www.ibtimes.co.uk/op-icarus-anonymous-launches-ddos-attacks-8-international-banks-1558987

Chellaney, Brahma. 2013. "China's salami-slicing strategy." *Washington Times*, August 6, 2013. https://www.washingtontimes.com/news/2013/aug/6/chellaney-chinas-salami-slicing-strategy/

Crosman, Penny. 2015. "Banks lose up to $100K/hour to shorter, more intense DDoS attacks." *American Banker*, April 23, 2015. https://www.americanbanker.com/news/banks-lose-up-to-100k-hour-ro-shorter-more-intense-ddos-attacks

Cybersecurity Association of Maryland, Inc. 2016. "The top 10 cybersecurity threats for financial institutions." March 2, 2016. https://www.mdcyber.com/blog/top-10-cybersecurity-threats-financial-institutions/

"Increasing number of financial institutions falling prey to cyber attacks." November 9, 2016. https://www.helpnetsecurity.com/2016/11/09/financial-institutions-cyber-attacks/

Kaspersky. 2017. "Cybersecurity in financial institutions 2016—And what 2017 holds." Kaspersky (blog), March 17, 2017. https://blog.kaspersky.com/from-the-perils-to-strategies/6682/

Khandelwal, Swati. 2016. “5 major Russian banks hit with powerful DDOS attacks.” *The Hacker News*, November 11, 2016. https://thehackernews.com/2016/11/bank-ddos-attack.html

Kitten, Tracy. 2015. “DDoS attacks against banks increasing.” *Skyebox Security*, August 24, 2015. http://www.bankinfosecurity.com/ddos-a-8497

Sarma, Ripunjoy Kumar. 2005. “How to get rid of a salami attack?” *The Economic Times*, June 23, 2005.

SecurityScorecard. 2016. “2016 Financial industry cybersecurity report.” https://media.scmagazine.com/documents/249/securityscorecard_2016_financi_62124.pdf

“Varonis predicts IT will face salami attacks in 2013.” 2012. *Varonis*, November 27, 2013. http://ir.varonis.com/news-releases/news-release-details/varonis-predicts-it-will-face-salami-attacks-2013

BIOMETRICS

The use of fingerprints to authenticate the identity of an individual is referred to as biometrics. It is the reliance on human characteristics that are unique to each individual and are difficult to copy or reproduce. It has been defined as “the automated means of recognizing a living person through the measurement of distinguishing physiological or behavioral traits” (United Kingdom Biometrics Working Group, 2002, p. 4). For biometrics to work, an individual must provide the characteristic, such as a fingerprint. The print is held then in a dataset. Because it is so difficult to duplicate these traits, and they are accurate, they provide a secure method for identifying people.

For example, visitors to Walt Disney World are required to place their fingers on a reader, which then scans and assigns a number to each person’s fingerprint. Each time the visitor re-enters the park, or visits another park, they tap their card and place their finger on the scanner. Park officials say this is done to verify the identity of the guest, which makes the process for entering the park easier and quicker, and also helps to ensure that passes are not being used by individuals who are not the owner.

The components of biometrics have been used for many years. The U.S. government began using facial recognition tools in the 1960s, and in the 1970s, speech components were being used to identify people. In 1986, the technology had expanded to use iris identification. The use of biometrics in security is a relatively new field, but it is growing in popularity. It is being used by companies that require high levels of security, such as airports. Even Apple has the home button fingerprint sensor, which they installed on their phones in 2013. Biometrics can be an accurate way to authenticate online consumers and reduce fraud.

The use of biometrics can be much more efficient than current methods for identifying individuals. Once a person is enrolled in the program, a large number of people can be processed very quickly, as there is no need to check a paper identification. A person’s identity can be verified much more quickly than using cards or IDs.

Fingerprints are not the only trait that can be used to validate a person’s identity, although, because they are cheap to collect and use, they are the most common.

Other physical and behavior traits can be hand or palm prints (length of fingers, lines in the palm), facial patterns, retina and iris scans (that measure the ring of color around the pupil), voice patterns, signatures (writing patterns), DNA, or even walking patterns. Data on these traits are painless to collect. Some companies and agencies are now using selfies as a way to identify their employees. Software will measure facial features, such as the length of a nose or size of the chin, and convert that into a unique code. The tax departments in Georgia and Alabama required those who filed their taxes to authenticate their tax returns with a selfie. Facial recognition biometrics can be used without the individual's knowledge. Thus, it is used at casinos to identify scammers or in airports to identify potential terrorists.

For some, the mass collection of individual, personal characteristics raises issues of privacy. Many people have concerns that the information will be collected and maintained without the individual's knowledge or permission. That information could then be used for many reasons other than what was originally intended. The data could be shared with other agencies or even to track people's movements. In short, the information may be misused (Smith, 2007).

Because of these concerns, some people may not want to provide their data to an organization. There may also be some people who are unable to provide the necessary data and are unable to enroll for some reason. Biometrics are also not a foolproof method for identifying individuals. Although it is rare, there are times when there is a false match. Conversely, criminals or those seeking to fool the system can use a fake finger made of latex to get around the system, or a voice recording. A program may not match a person with a selfie photo if the lighting is different, or if the individual has lost a significant amount of weight.

Another concern with biometrics revolves around the security of the dataset. If there is one dataset that includes a series of biometric data, it may become a high-profile target for hackers or an internal theft by an angry employee. This happened in 2014, when unknown hackers (likely from China) were able to steal 5.6 million fingerprints of both current and former federal employees from the U.S. Office of Personnel Management. Most officials would agree that there is a possibility that biometric data could be misused, just like any other form of identification.

See also: Prevention

Further Reading

Barton, Bruce, Shane Byciuk, Collin Harris, Damian Schumack, and Kevin Webster. 2005. "The emerging cyber-risks of biometrics." *Risk Management*, 52, 9: 26–31.

Glaser, April. 2016. "Biometrics are coming, along with serious security concerns." *Wired*, March 9, 2016. https//www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/

Smith, Russell. 2007. "Biometric solutions to identity-related cybercrime." In *Crime online*, edited by Yvonna Jewkes. Devon, UK: Willan Publishing, pp. 44–59.

Thadani, Trisha. 2016. "Companies try out selfies as password alternatives; facial-recognition apps use smartphone snapshots to verify identity of customers, taxpayers." *Wall Street Journal*, October 17, 2016. https://www.wsj.com/articles/companies-try-out-selfies-as-password-alternatives-1476661046

United Kingdom Biometrics Working Group. 2002. "Use of biometrics for identification: Advice on product selection." http://www.cesg.gov.uk/site/ast/biometrics/media/Biometrics%20Advice.pdf

United States General Accounting Office. 2002. "Technology assessment: Using biometrics for border security, GAO-03-174." November 2002. http://www.gao.gov/new.items/d03174.pdf

Woodward, John D., Jr., Nicholas M. Orlans, and Peter T. Higgins. 2003. *Biometrics*. Berkeley, CA: McGraw-Hill.

BITCOIN

Bitcoin is a digital currency considered to be the first cryptocurrency, or digital currency operating in a decentralized system. This means that Bitcoin exchanges can take place without the use of a centralized entity to verify the transaction. Rather, transactions are verified through members of the Bitcoin community, referred to as miners. The record of these verified transactions is known as a blockchain and is available to the public. Bitcoin is also the largest cryptocurrency in terms of market capitalization (Hileman and Rauchs, 2017) with the current value of over $100 billion (Bitcoin, 2018).

A person using the name Satoshi Nakamoto created Bitcoin in 2009. In January of that year, Nakamoto sent the first Bitcoins to Hal Finney (Peterson, 2014). As of this writing, Nakamoto's identity remains a mystery. Nakamoto disassociated from Bitcoin in 2010 (Bitcoin, 2018).

When Nakamoto created Bitcoin, he introduced the concept of blockchains, a decentralized public string of data entries, with the entries connected via cryptography. With Bitcoin, the string of data entries is a ledger of Bitcoin transactions. Where blockchains are public, they can be checked for accuracy by numerous, unrelated individuals; these individuals are known as "Bitcoin miners." The idea is that if multiple people check and verify the accuracy of blockchains, any attempts to fraudulently alter the blockchain can be easily discovered and rectified. By doing this, cryptocurrencies can remain decentralized. There is financial incentive to mine Bitcoin. For each block (a section of transactions in the overall blockchain) mined, a Bitcoin miner currently receives 12.5 Bitcoin. Other cryptocurrencies besides Bitcoin use blockchains as well. Some of those cryptocurrencies essentially copy the blockchain system employed by Bitcoin, while others build on the initial blockchain concept introduced by Bitcoin in innovative ways (Hileman and Rauchs, 2017).

While blockchains appear to solve the problem cryptocurrencies faced when trying to create a decentralized monetary system, blockchains are not without their own problems. The ability of blockchains to maintain the integrity of a cryptocurrency is dependent upon the honesty of the miners verifying those blockchains. While incentive to maintain the integrity of the blockchains is provided to miners in the form of actual Bitcoin, it has been argued that this may not be enough incentive to prevent fraud in the verification of blockchains (Eyal and Sirer, 2018).

Bitcoin, as well as other cryptocurrencies, are prohibited in several countries. In some countries, this ban is explicit, such as in Bolivia, Egypt, and the United Arab Emirates. In others countries, such as in China, Iran, and Columbia, there is not an out-and-out ban on citizens utilizing cryptocurrencies, but financial institutions within the country are barred from using them, essentially amounting to a ban (see Law Library of Congress, 2018). Cryptocurrencies are, however, currently legal in the United States. Indeed, the first commercial Bitcoin transaction took place in the United States from the United Kingdom. On May 22, 2010, Laszlo Hanyecz, who lived in Florida, offered to pay 10,000 Bitcoins to anyone on an online forum who would buy him pizza. Another forum user in the United Kingdom accepted the offer and ordered two pizzas for Hanyecz from a Papa John's in Hanyecz's area (Bort, 2014). Presently, several businesses in the United States accept Bitcoin, including Microsoft, Subway, and Expedia (Chokun, 2018).

While the use of Bitcoin is legal in the United States, there are ways Bitcoins are used to facilitate criminal acts. Because Bitcoin cannot be directly traced back to an individual, it can be used to pay for illegal goods or services. One study estimated that half of the transactions conducted using Bitcoin involve illegal activity and that a quarter of all Bitcoin users have used it for illegal purposes (Foley et al., 2018).

The process of mining Bitcoin has also come under fire because it requires an extensive amount of electricity. Not only are transactions in the blockchain verified by multiple users, but the process of deciphering the cryptography involved with a transaction draw a fair amount of power. Because so much electricity is required to maintain a blockchain, it is argued that Bitcoin and other cryptocurrencies are not feasible as a replacement for traditional currency (Shin, 2018). It is not just the cost of electricity use associated with transaction verification that makes it unfeasible—the environmental impact of such heavy use of electricity is substantial. It is estimated that the electricity used to mine Bitcoin is similar to the amounts used by some countries, such as Hungary, New Zealand, Peru, and Switzerland (Hern, 2018; Shin, 2018). Generating that much electricity is estimated to produce 20 megatons of CO_2 emissions annually (Hern, 2018).

This problem could be compounded if Bitcoin or another cryptocurrency were to replace traditional currency. The mining of Bitcoin is a competitive process, where those who are able to mine faster are more likely to reap the financial benefits of mining. Those with more processing power have an edge, but that will cost more electricity. At a certain point, it no longer becomes economically advantageous to increase processing power because the cost of the electricity usage required to utilize it offsets the profits to be made. If Bitcoin were the traditional currency, however, the value of Bitcoin would likely go up. This, in turn, would increase the amount of electricity one could use to mine Bitcoin and still have it be profitable (Hern, 2018). This would result in even more CO_2 emissions.

See also: Cryptocurrency; Digital Currency; Nakamoto, Satoshi; Silk Road

Further Reading

Bitcoin. 2018. "Frequently asked questions." Bitcoin.org. https://bitcoin.org/en/faq#general

Bort, Julie. 2014. "May 22 is Bitcoin pizza day thanks to these two pizzas worth $5 million today." *Business Insider*, May 21, 2014. https://www.businessinsider.com/may-22-bitcoin-pizza-day-2014-5?IR=T

Chokun, Jonas. 2018. "Who accepts Bitcoins as payment? List of companies, stores, shops." 99Bitcoins, September 13, 2018. https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/

Eyal, Ittay, and Emin Gün Sirer. 2018. "Majority is not enough: Bitcoin mining is vulnerable." *Communication of the Association for Computing Machinery* 61, 7, pp. 95–102.

Foley, Sean, Jonathan R. Karlsen, and Tālis J. Putniņš. 2018. "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?" *Social Science Research Network*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645

Hern, Alex. 2018. "Bitcoin's energy usage is huge—We can't afford to ignore it." *The Guardian*, January 17, 2018. https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency

Hileman, Garrick, and Michel Rauchs. 2017. *Global cryptocurrency benchmarking study*. Cambridge, UK: Cambridge Centre for Alternative Finance.

Law Library of Congress. 2018. *Regulation of cryptocurrency around the world*. Washington, D.C.: The Law Library of Congress.

Nakamoto, Satoshi. 2008. "Bitcoin: A peer-to-peer electronic cash system." https://bitcoin.org/bitcoin.pdf

Peterson, Andrea. 2014. "Hal Finney received the first Bitcoin transaction. Here's how he describes it." *Washington Post*, January 3, 2014. https://www.washingtonpost.com/news/the-switch/wp/2014/01/03/hal-finney-received-the-first-bitcoin-transaction-heres-how-he-describes-it/?utm_term=.82ddd0bb27d8

Shin, Hyun Song. 2018. "Cryptocurrencies: Looking beyond the hype." In *Bank for International Settlements Annual Economic Report*. Basel, Switzerland: Bank for International Settlements.

BLACK-HAT HACKERS

A black-hat hacker is a person who has extensive knowledge of computers and networks and who uses the knowledge to hack into the computer systems of government offices or companies. They are able to bypass network security to access the computers or systems. Once there, a black hat will upload malware or viruses that allow them to steal online data, information or communications, or conduct phishing scams. In some cases, black hatters have stolen data, shut down entire networks, or altered a system in some way that causes harm.

Black-hat hackers are often motivated to do this kind of work by the personal financial gain they may achieve if they are able to steal money from a victim, or steal another person's information to purchase goods, or even sell them on the black market. They are sometimes motivated by a particular cause—some black-hat hackers may oppose an agency or organization or have some kind of vendetta against them. These hackers are, in some cases, disgruntled employees. Another motivation is political: they may oppose an organization's political activities or ideologies. Some hackers simply have malicious intent. They seek to cause damage and want to see how much harm they can accomplish.

Despite their reputation for being "bad guys" or cybercriminals, many people seek to become black hatters. There are events where interested people can learn skills needed to do this. DEF CON, founded in 1993 by Jeff Moss, a former computer hacker turned security expert, is currently the largest hacking conference. Attendees, who include both hackers and law enforcement officers, learn about trends in hacking tools and techniques. Another event is Black Hat USA, a conference started in 1997 by Moss, where individuals who attend are able to learn about trends in security risks and new research and development for offensive and defense hackers. The conference provides a great deal of hands-on training for attendees, who are a mix of hackers, law enforcement, government, and officials from private organizations. This can be anyone interested in hacking or prevention of hack behaviors.

One well-known black hatter is Kevin Poulsen, also known as Dark Dante. Poulsen gained his fame as a black hatter after he illegally accessed the telephone lines of W-KIIS, a radio station from Los Angeles. He became the winning caller to a call-in contest and acquired a Porsche 944. After his hacking became evident, he went into hiding but was eventually captured by the FBI in 1991. He pleaded guilty to mail, wire, and computer fraud; money laundering; obstruction of justice; and obtaining information on covert businesses run by the FBI. The court sentenced him to spend four years and three months in prison and required him to pay a fine of $56,000. Poulsen now works for *Wired News*, a computer-related journal. He also assisted law enforcement in identifying sex offenders on the former social media platform MySpace.

Another well-known black-hat hacker is Albert Gonzalez. He was responsible for stealing information on 170 million credit card and ATM card numbers and then selling them online for a profit. This was the largest theft in history. After his arrest in 2008, Gonzalez helped the FBI through Operation Firewall that resulted in the arrest of 28 hackers.

Andrew Auernheimer is also known as a black-hat hacker. In 2010, he was in a group that hacked into the computer systems of AT&T, stealing information from 114,000 iPad users and posting the information online.

See also: Auernheimer, Andrew Alan Escher; DEF CON; Hacker and Hacking; Poulsen, Kevin; White-Hat Hackers

Further Reading

Suddath, Claire. 2009. "Master hacker Albert Gonzalez." *Time*, August 19, 2009. http://content.time.com/time/business/article/0,8599,1917345,00.html.

Verini, James. 2010. "The Great Cyberheist." *New York Times*, November 10, 2010. https://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html.

"Welcome to Black Hat USA." 2018. https://www.blackhat.com/us-18/

Xu, Zhengchuan, Qing Hu, and Chenghong Zhang. 2013. "Why computer talents become computer hackers." *Communications of the ACM* 54, 4 (April): 64–74.

Zetter, Kim. 2016. "Hacker Lexicon: What are white hat, gray hat, and black hat hackers?" *Wired*, April, 13, 2016. https://www.wired.com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers/

BLANKENSHIP, LOYD (1965–)

Loyd Blankenship is a computer hacker who is also known as the Mentor. In 1986, when he was 21, he was arrested for "being in a computer [he] shouldn't have been" and decided to write an essay to describe the thoughts and goals of a hacker. The piece was called "The Conscience of a Hacker," later to become known as the Hacker Manifesto. The treatise was published in the seventh issue of the magazine *Phrack*, a publication for hackers and others interested in computer technology. The Manifesto continues to be a valid description of the hacking culture. In fact, a poster of the Manifesto appears in the film *The Social Network* (2010), hanging in Mark Zuckerberg's dorm room. The document was read in the movie *Hackers* (1995), and Blankenship receives credit for it in the movie's credits.

Blankenship was a member of various hacking groups, including LoD, Extasy Elite, Racketeers, and the PhoneLine Phantoms. He authored the rulebook/toolkit for a role-playing game called *GURPS Cyberpunk*. In the manual, Blankenship described how players could break into a computer system if they wanted to steal, alter, or destroy information, or just to look at another's files. Agents in the U.S. Secret Service assumed the book was a guide to teach others how to carry out cybercrimes. On March 1, 1990, agents entered Blankenship's apartment and questioned him for hours about his role in computer hacking schemes.

That same day, agents raided the headquarters of Steve Jackson Games, where Blankenship worked. The Secret Service sought to search the computers of the company because they believed that information pertaining to stolen documents belonging to Bell South had been posted in the internet. The agents who performed the search took the *GURPS Cyberpunk* manuscript, thinking it would serve as evidence in a subsequent trial.

Jackson, the designer of the game *GURPS*, ended up suing the Secret Service for violation of various privacy laws, and the seized material was returned to the company. Blankenship's rulebook for the game was published by Steve Jackson Games and made available to the public. In the case that ensued, *Steve Jackson Games, Inc. v. United States Secret Service*, a federal court ruled for the first time that the Privacy Protection Act, passed by the U.S. Congress in 1980, applied to electronically stored information.

Blankenship has since retired and works as a freelance game developer and electronic musician.

See also: Legion of Doom

Further Reading

Blankenship, Loyd. 1986. "The conscience of a hacker." *Phrack Magazine* 1, 7, Phile 3 of 10.

Caparula, J. M., and Scott D. Haring. 1990. *GURPS horror: The complete guide to horrific roleplaying*, edited by Loyd Blankenship and Steve Jackson. Austin, TX: Steve Jackson Games.

Lewis, Peter. 1990. "The executive computer: Can invaders be stopped but civil liberties upheld?" *New York Times*, September 9, 1990. https://www.nytimes.com/1990/09/09/business/the-executive-computer-can-invaders-be-stopped-but-civil-liberties-upheld.html

McCubbin, Chris W. 1990. *GURPS fantasy folk: Fantastic races for fantasy roleplaying*, edited by Loyd Blankenship and Steve Jackson. Austin, TX: Steve Jackson Games.

Murphy, Katherine. 2017. "Hacking history: The Mentor and the Hacker Manifesto." Cybertraining 365 (Blog). April 9, 2017. http://blog.cybertraining365.com/2017/04/09/1014/

Perry, Gregory E., and Ballard Cherie. 1993. "A chip by any other name would still be a potato: The failure of law and its definitions to keep pace with computer technology." *Texas Tech Law Review*, 24, 797–830.

BLOCKCHAIN, *see* BITCOIN

BOTS AND BOTNETS

A bot is a type of software that can carry out tasks when commanded, or that can cause a computer to perform a task the user is not aware of. The word "bot" comes from the word robot, and it implies that a computer has become a robot—it has been programmed by someone other than the owner to do something. Some bots are useful, for example, a shopbot is a program that reviews retail sites and locates the store where the item is for sale at the cheapest price. Another example is a "knowbot" that collects information by visiting other sites to gather information.

However, bots can also be very damaging. A harmful bot can be uploaded to a computer to carry out a malicious act. Some may allow a hacker to remotely take control of a computer so it does things for the hacker. It may force a computer to send large numbers of spam e-mails to a website as part of a DoS attack, forcing the site to slow down or be shut down. It may infect the machine with other malware that allow criminals to steal personal information or data so they can steal the computer owner's identity. Offenders may seek to gain unauthorized access to a system in order to steal business secrets. It can also send out spyware that will collect information about the user's activities and send that to the hacker. Once infected with a bot, the machine is referred to as a "zombie."

All computers are at risk of becoming bots, including those owned by individuals, companies, organizations, governments. They can even affect personal devices and smartphones. This means that millions of unsuspecting users are at risk of becoming victims.

Often, hackers will attempt to network huge numbers of infected computers (a few hundred or even thousands of infected machines) at one time. This way, the hacker will have control of multiple machines at one time, allowing the hacker to carry out large-scale attacks. It is more effective to steal large amounts of data when many machines are under a hacker's control. When a large amount of zombie computers are commanded at once, the network is known as a "botnet." This comes from the words "robots" and "networks." Sometimes a botnet is called a "zombie army." The person who is in control of the botnet is referred to as a "bot herder" or "bot master."

Once the hacker creates a botnet, it can be rented to others or loaned out to others who want to control the computers for some reason. The price the hacker charges will depend on the number of computers that make up the botnet or the amount of time the offender needs to use the botnet.

One famous botnet attack was named Zeus and was detected in 2009. This software relied on a form of malware called a Trojan horse to seek out vulnerable computers and infect them to create thousands of zombie computers. Once the botnet was formed, it was used to attack banking and other financial organizations to allow the hackers to steal financial information from both individuals and companies. The bot was sent through a phishing e-mail and asked victims for their personal information. When a victim opened the e-mail, the machine they were using was then infected with the malware. In more recent years, the bot has been used as a way to spread ransomware that locks a victim's computer until a ransom fee is paid. This botnet later became known as the Gameover Zeus, which relied on peer-to-peer networks to disseminate itself. Although the creator of the malware claims to have retired the program, many experts believe it is still active.

Another famous botnet, Srizbi, began to emerge in 2007. Srizbi sent e-mails to a large number of voters as a way to convince them to vote for Republican presidential candidate Ron Paul in 2008. Because of that, the botnet was often referred to as the Ron Paul spam botnet.

In 2016, a botnet referred to as Mirai attacked Dyn, a company that helps provide support for the internet. This malware attacked internet routers and cameras, using default usernames and passwords that are set by manufacturers to install malware. The attack was then executed out by a botnet of zombie computers that were programmed to carry out a DDoS attack, overwhelming the company and causing the internet to shut down for a short time for millions of users around the world.

Most computer owners do not realize that their computer has been infected with a bot and are unaware that anything is wrong. The owner is still able to use the computer, and it seems to be working fine, except it may be operating a little slower than before. Most botnets have a small "footprint" so that they use system resources but are difficult to recognize. This means that the malware is not detected by the owner for a long period, giving the offender the potential to cause a great deal of damage to a system or steal a large amount of data.

When a hacker seeks to infect computers to make bots and botnets, they create a malware that is able to scan the internet to find vulnerable computers. Many computers and systems are not adequately protected against malware, so they are easy to locate and infect. It only takes a few minutes for a computer or smartphone to become infected. The malware will attempt to infect the largest number of computers possible.

To prevent a computer from becoming a bot, it is important to keep updated security antivirus programs updated. It is also important for a user to refrain from opening attachments unless the sender is a recognized entity. Users should also change default usernames and passwords on new devices. Once a vulnerability is identified, it should be patched as quickly as possible.

See also: Distributed Denial-of-Service Attack (DDoS); Malware; Ransomware; Trojan Horse

Further Reading

Hay Newman, Lily. 2016. "The Botnet that broke the internet isn't going away." *Wired*, December 9, 2016. https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/

Lee, Timothy B. 2013. "How a grad student trying to build the first botnet brought the internet to its knees." *The Washington Post*, November 1, 2013. https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/?utm_term=.0b76f3d3cd54

Schiller, Craig A., Jim Binkely, David Harley, Gadi Evron, Toni Bradley, Carsten Willems, and Michael Cross. 2007. *Botnets: The killer web app*. Burlington, MA: Syngress.

Tiirmaa-Klaar, Heli, Jan Gassen, Elmar Gerhards-Padilla, and Peter Martini. 2013. *Botnets*. New York: Springer.

Wenke Lee, Cliff Wang and David Dagon. 2008. *Botnet detection: Countering the largest security threat*. New York: Springer.

BYPASS

In general, a bypass is an alternate route of getting to a destination. In the cybercrime context, a bypass specifically refers to an alternate route taken around the security measures in place on a computer or network. This is generally done by exploiting some flaw in those security measures.

It is possible to bypass a computer's or network's security measures in several ways. One way would be to elicit a user's password from them. This could be accomplished via phishing or a similar method. Another way to bypass security measures would be to use spyware to obtain a user's password. Not all methods of bypassing security measures require a perpetrator to obtain a user's password. A hacker might be able to find a way to bypass the entire password authentication process.

Although the use of bypasses is often unauthorized, this does not mean that all use of bypasses is unauthorized. Intentional bypasses—referred to as backdoors—are sometimes used to allow network administrators and others to access certain parts of the network walled off to the general public. Law enforcement might also attempt to bypass security measuring in place on a computer or similar device. This happens in drug-trafficking cases. If a drug trafficker is caught and has a cell phone in their possession, law enforcement will generally want to search that phone for pertinent information relating to the drug distribution network within which the apprehended drug trafficker is working. If the phone is protected by a password, law enforcement has to find a way to obtain the password or to bypass the password requirement. This could be done in other criminal cases as well where evidence of a crime is believed to be on a computer or similar device. For example, in cases involving child pornography, a suspect may have their computer password protected for the specific purpose of preventing others from accessing those images.

Generally, law enforcement will have tools at their disposal to allow them to bypass security measures on electronic devises. However, this may not always the case. One prominent example of this involved the FBI and Apple. In 2015, Syed Rizwan Farook and Tashfeen Malik carried out a terrorist attack in San Bernardino, California, that left 14 civilians dead. As part of the FBI's investigation, it retrieved several cell phones. The FBI claimed to be unable to bypass the security measures on one of those cell phones—an iPhone made by Apple. It appears that law enforcement believed the cell phone could contain information about a possible third shooter (Ferran and Date, 2016). In 2016, the FBI filed an order to compel Apple to assist the FBI in bypassing the security measures on the phone. Apple refused.

Before the court could rule on the case, the FBI ultimately asked that their motion be vacated after bypassing the security measures on the phone using a third party (Selyukh, 2016). While this resolved the legal dispute between the FBI and Apple, the question as to whether the government should be able to compel a private technology company to build in a bypass for them still remains. Apple did not believe it should, calling it an overreach by the government (Cook, 2016). To further complicate matters, a report by the U.S. Office of the Inspector General (2018) found that the entire lawsuit was perhaps unnecessary. The method that was ultimately used to bypass the security measures of the cell phone could likely have been discovered sooner but for a lack of communication within the FBI.

See also: Backdoor; Child Pornography; Drug Trafficking; Encryption; Federal Bureau of Investigation; Hacker and Hacking; Phishing; Spyware; Vulnerability

Further Reading

Cook, Tim. 2016. "A message to our customers." Apple, February 16, 2016. https://www.apple.com/customer-letter/

Ferran, Lee and Jack Date. 2016. "San Bernardino DA: Clues to unconfirmed 3rd shooter, 'cyber pathogen' could be on iPhone." *ABC News*, March 4, 2016. https://abcnews.go.com/US/san-bernardino-da-clues-unconfirmed-3rd-shooter-cyber/story?id=37399545

Office of the Inspector General. 2018. *A special inquiry regarding the accuracy of FBI statements concerning its capabilities to exploit an iPhone seized during the San Bernardino terror attack investigation*. Washington, D.C.: Office of the Inspector General.

Selyukh, Alina. 2016. "The FBI has successfully unlocked the iPhone without Apple's help." *National Public Radio*, March 28, 2016. https://www.npr.org/sections/thetwo-way/2016/03/28/472192080/the-fbi-has-successfully-unlocked-the-iphone-without-apples-help

C

CALCE, MICHAEL (1986–)

Michael Calce, also referred to as Mafia Boy, is a hacker known for a series of denial-of-service (DoS) attacks in 2000 against large companies, including Yahoo, Amazon, Dell, eBay, and CNN. After pleading guilty to multiple criminal charges, Calce became a computer security expert who advises companies on ways to improve their cybersecurity.

Born in 1986 in West Island, Quebec, Calce received his first computer at the age of six from his father and became obsessed with how they worked. At age 15, Calce said he downloaded a security tool from a file-sharing platform, typed in some addresses of major companies, and left the program running while he went to school. The program carried out DoS attacks, which overloaded servers so that they became unresponsive. The program ran the attacks all day long, causing Yahoo to shut down for about an hour. Calce said he was unaware of what he had done until he heard about the results on the news later that day. It has been estimated that his actions caused about $1.7 billion in damages.

After the attacks, Calce wrote about his actions in chatrooms. Officials from the FBI and the Royal Canadian Mounted Police became aware of him and arrested Calce in April 2000. Calce admitted that his goal was simply to intimidate other hacker groups, not necessarily to cause harm to the companies he hacked. Calce was charged with committing 56 computer-hacking crimes, and he eventually pleaded guilty to the majority of the charges. In 2001, he was sentenced to eight months of "open custody," which he served in a group home. His sentence also included one year of probation and a fine. The court also restricted his access to and use of the internet.

The attacks brought attention to the fact that a young boy was able to easily hack into the computer systems of major international corporations, underscoring the need for greater security to protect computer security. The attack gained such notoriety that President Bill Clinton decided to create a cybersecurity working group that would make recommendations to strengthen cyber laws in the United States.

Since then, Calce has become a white-hat hacker and works for different companies to help with their network security needs. He owns a company in Canada that works to identify weak points in their computer networks (vulnerabilities). He has also written books about his experiences as a hacker. In recent interviews, Calce has noted that most computer systems are not secure, mostly because technology is improving so quickly that it is tough to keep systems safe. He has a general distrust of online banking systems and refuses to use a debit card because of the ease by which a criminal can steal passwords.

See also: Denial-of-Service Attack (DoS); Hacker and Hacking; President and Cybercrime; White-Hat Hackers

Further Reading

Calce, Michael, and Craig Silverman. 2008. *Mafiaboy: How I cracked the internet and why it's still broken*. Toronto: Penguin Group Canada.

Calce, Michael, and Craig Silverman. 2009. *Mafiaboy: A portrait of the hacker as a young man*. Toronto: Viking Canada.

Gross, Doug. 2011. "'Mafiaboy' breaks silence, paints 'portrait of a hacker.'" CNN, August 15, 2011. www.cnn.com/2011/TECH/web/08/15/mafiaboy.hacker/index.html

Hersher, Rebecca. 2015. "Meet Mafiaboy, the 'bratty kid' who took down the internet." National Public Radio, February 7, 2015. https://www.npr.org/sections/alltechconsidered/2015/02/07/384567322/meet-mafiaboy-the-bratty-kid-who-took-down-the-internet

McMillan, Robert. 2008. "Mafiaboy grows up: A hacker seeks redemption." *Computer World*, October 13, 2008. https://www.computerworld.com/article/2533517/networking/mafiaboy-grows-up--a-hacker-seeks-redemption.html

Middleton, Bruce. 2017. *A history of cyber security attacks: 1980 to present*. Boca Raton, FL: CRC Press.

CAN-SPAM ACT OF 2003

Senators Conrad Burns (R-MT) and Ron Wyden (D-OR) sponsored the Controlling the Assault of Non-Solicited Pornography and Marketing Act, or CAN-SPAM Act, which President George W. Bush signed in December 2003. The new law aimed to prevent the spread of spam, or unsolicited junk e-mail sent in bulk, across computers. This would be done by placing regulations on the e-mails that are sent to individual e-mail address and allowing for easy "opt out" procedures for those who do not want to receive additional spam messages.

As defined in the Act, spam is "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service." Spam e-mails typically appear in inboxes of internet users that can quickly fill up inboxes. Besides being annoying, spam can cause significant damage. They are often used to spread malware that allows a criminal to steal personal data or even cause damage to a company's computer network.

The CAN-SPAM Act created new rules regarding these unsolicited commercial e-mail messages. These e-mails must be identified as a spam advertisement or solicitation so the recipient is aware of the nature of the message. The law requires that the header or subject line of a spam e-mail not be misleading or contain deceptive information that encourages a user to open it.

Those who receive the e-mails must be given "clear and conspicuous" instructions on how to opt-out of additional e-mails or request that they not receive any further messages from the company. The e-mails must include a return e-mail address that the recipient can use to indicate their intention that they no longer receive additional e-mails. The opt-out request must be implemented within 10 business days of the request, and a fee cannot be charged to a recipient who seeks to unsubscribe. Once that opt-out request has been received, no additional spam messages can be sent. The spam e-mail must also contain a valid, physical postal address for the sender.

If a company continues to send the e-mails or violates any provisions of the law, they face possible penalties for "unfair or deceptive acts." If convicted under the law, an offender could be fined up to $16,000 for each e-mail or message sent that was in violation of the law.

The proposed law had support from some of the biggest e-mail providers, including America Online, Microsoft, and Yahoo. Supporters of the law proposed that the FTC establish a "do not e-mail" registry, but the proposal was scrapped when critics complained that the list would give potential spammers an inventory of confirmed e-mail addresses.

Opponents of the law complained that it would not be effective in fighting spam. They pointed out that it is often difficult to track down or identify the sender of a deceptive or harmful spam message. Further, the law only regulates commercial e-mails but does not limit noncommercial bulk e-mails that users may receive. Some critics believed that recipients of spam should be given an option to sue those who sent the unwanted e-mails, which was not included in the law. Opponents also complained that the bill did not include a provision to simply prohibit companies from sending e-mail spam, even though many states had such legislation in effect. They complained that the CAN-SPAM Act would prohibit states from passing additional protections against spam.

In the months after President Bush signed the law, officials at the FTC reported a decrease in spam e-mails that were sexually explicit. However, most other agencies agreed that the amount of spam e-mails rose in the year after the law was passed.

The first person to be arrested under the Act was Anthony Greco, an 18-year-old from Cheektowaga, New York. In 2004, the social networking site MySpace asked Greco to write a computer program so they could send users ads for adult websites and mortgage refinancing. Greco created 27,000 fake accounts in order to send nine million spam messages to users (in this case "spim," or unwanted messages that are sent through instant messaging). He then tried to blackmail MySpace officials by demanding that he be hired permanently or he would tell others about how he sent the spam e-mails. MySpace officials spent over $20,000 to delete the spam messages and responding to user complaints. Greco was arrested on February 16, 2005, pleaded guilty, and was sentenced to 18 to 24 months in prison.

In 2008, Robert Soloway, also known as the "Spam King," was sentenced to spend 47 months in a federal prison after he sent tens of millions of unsolicited spam e-mails in violation of the CAN-SPAM Act. He was also sentenced to pay $708,000 in restitution to victims. Soloway was charged with fraud, money laundering, and identity theft, but he was known for sending large amounts of spam that he labels as "opt-in" services. He has been sued by Microsoft and other large companies for his activities. He has been ordered by a U.S. District Judge from sending any spam e-mails.

In July 2014, legislators in Canada passed a similar law, the Canadian CAN-SPAM Act, requiring any e-mail messages sent in Canada to follow similar rules.

See also: E-mail-related Crimes; Malware; President and Cybercrime

Further Reading

Federal Communications Commission. "CAN_SPAM." https://www.fcc.gov/general/can-spam

Ford, Roger Allan. 2005. "Preemption of state spam laws by the federal CAN-SPAM Act." *The University of Chicago Law Review*, 72, 1: 355–384.

Gaither, Chris. 2004. "Can spam be canned? Senders of mass junk e-mail have proved to be a resilient bunch, exacting revenge on the software makers that want to put the out of business." *Los Angeles Times*, May 23, 2004. http://articles.latimes.com/2004/may/23/business/fi-spam23

Hansell, Saul. 2003. "Finding solution to secret world of spam." *New York Times*, May 5, 2003. https://www.nytimes.com/2003/05/05/business/finding-solution-to-secret-world-of-spam.html

McGuire, David. 2005. "A year after legislation, spam still widespread; technology seen as best deterrent." *The Washington Post*, January 4, 2005. www.washingtonpost.com/wp-dyn/articles/A46037-2005Jan3.html

"Spammer Gets Likely Prison Sentence." 2005. *Fox News*, October 18, 2005. www.foxnews.com/story/2005/10/18/spammer-gets-likely-prison-sentence.html

CAPITAL ONE BREACH

In March 2019, a computer hacker was able to access the personal information of 100 million people across the United States and 6 million customers in Canada who applied for credit cards with Capital One between 2005 and 2019. The customers were both individual consumers and small businesses. The information accessed included account information, Social Security numbers, addresses, credit scores, and other sensitive data. The breach was detected in July.

It wasn't long before the offender was identified by law enforcement. The offender was Paige Thomas, a 33-year-old woman who used the online name "erratic." Thomas had been a tech company software engineer for Amazon Web Services and had excellent computer skills. In the past, she helped to create a group on Meetup called Seattle Warez Kiddies for people who had an interest in programming, hacking, and cracking. She described her intentions to set up a "hack night" for anyone who was interested.

Law enforcement officials had little trouble identifying Thomas as the Capital One hacker. She bragged about the hack on social media, describing how she was able to carry out the attack. Someone immediately contacted Capital One to notify them of a GitHub page that contained the personal data. Thomas also described her hacking on Twitter. She wrote, "I wanna get it off my server, that's why I'm archiving all of it, lol." She also wrote, "It's all encrypted. I just don't want it around, though" (Brandom, 2019). Thomas was arrested at her home in Seattle and later charged with computer fraud and abuse, an offense that is punishable by up to five years in prison and a $250,000 fine if found guilty. Thomas was held at the Federal Detention Center in SeaTac while awaiting trial.

The 2019 Capital One breach was one of the largest hacks of the financial sector, but it does not appear to be one of the more damaging hacks. There is no evidence that Thomas sold any of the information she had or released it in any way. Nonetheless, officials at Capital One reported the incident to federal law enforcement agencies immediately and cooperated with them to identify the extent of the breach as well as the identity of the offender. The chairman and CEO of the company, Richard Fairbank, immediately apologized to consumers. All customers who were at risk of having their personal information stolen were identified via a letter. Capital One promised free credit monitoring services to victims. It was estimated that the hack will cost the company up to $150 million to notify customers, to pay for credit card monitoring, and for legal support.

Cybersecurity professionals suggested that in order to prevent any further harm, victims should immediately freeze their credit to prevent anyone from opening a credit card or loan in the victim's name. Experts suggested that possible victims add additional security to their accounts (i.e., stronger passwords), and use the free credit monitoring to watch for unauthorized credit card purchases or other suspect activity.

The company quickly discovered that they had an improperly configured firewall that allowed Thomas to gain access. The firewall was patched immediately to prevent further hacking. New York Attorney General Letitia James began an investigation into the crime as a way to ensure that the crime would be solved and the offender punished. In response, Senator Ron Wyden, a Democrat from Oregon, proposed a new bill in Congress that would establish stricter protections for consumers' personal information. The bill, called the Consumer Data Protection Act of 2018, would increase punishments for anyone who used customer data for criminal activities. In addition, new punishments were proposed for senior officials who did not follow rules on data use. Those punishments would result in prison terms of 10–20 years. Wyden's bill would also establish a Do Not Track list that would give consumers the right to stop companies from sharing their personal data with third parties.

The 2019 hack was not the first time Capital One had experienced a breach. In 2017, Capital One issued letters to customers affected by a breach committed by a company "insider." This time, there was unauthorized activity that occurred for four months in early 2017: an employee, who was later fired from the company, examined customer records without permission. Many of the records contained personal, sensitive information such as account numbers, Social Security numbers, and birthdates. Because the employee had no purpose for looking at the records, company officials assumed they were attempting to steal information, possibly to sell the information for profit. Company executives offered to provide two years of free credit monitoring services to those affected.

In 2014, Capital One notified customers that their personal information may have been accessed by an employee who was later fired. The company apologized and offered two years of identity protection services to any customer whose information was part of the breach.

See also: Banking Attacks; Hacker and Hacking; Identity Theft

Further Reading

Brandom, Russell. 2019. "The Capital One breach is more complicated than it looks." *The Verge*, July 31, 2019. https://www.theverge.com/2019/7/31/20748886/capital-one-breach-hack-thompson-security-data.

Capital One. 2019. "Information on the Capital One cyber incident." August 4, 2019. https://www.capitalone.com/facts2019/

Flitter, Emily, and Karen Weise. 2019. "Capital One data breach compromises data of over 100 million." *New York Times*, July 29, 2019. https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html

Goldman, Jeff. 2014. "Capital One acknowledges insider breach." eSecurityPlanet, November 5, 2014. https://www.esecurityplanet.com/network-security/capital-one-acknowledges-insider-breach.html

Identity Theft Resource Center. 2017. "Capital One reports inside job data breach." August 3, 2017. https://www.idtheftcenter.org/capital-one-reports-inside-job-data-breach/

CARBERP

Carberp, which first appeared in the fall of 2010, is the name of a Trojan designed to target online banking and social media with the intent of stealing a people's banking information. Originally, it was used to steal money from banks located in Russia, allowing criminals to steal e-commerce payments from PayPal, e-banking, or debit cards. It is still most active in that country but has been used in the United States as well. Offenders using Carberp have stolen millions from banks since it was written (Krebs, 2013).

Carberp works by allowing the criminals to scan a victim's login data before it can be encrypted. The malware then sends the stolen information to the hacker's server, where they can view a victim's login information and password. At that point, the hackers can remotely control the login and any online transactions. In the end, a hacker is able to steal money from a bank account. Carberp also affects social media. In 2012 it blocked some users' access to Facebook. In December 2012, Carberp also attacked Google's mobile operating system, Android. The malware enabled cybercriminals to steal data from a victim's Gmail account or accounts with Google Photos, Google Docs, and Google Play.

In 2012, the creators of the malware offered to sell a new version of the program on an underground forum. They made the Trojan available for a monthly subscription costing between $2,000 and $10,000, or a flat fee of $40,000. Experts explain that the price for the malware is so high because the code is so well written. The authors of the malware were alleged to have been a group of hackers who worked on separate parts of the program and sent their work to a ringleader in Ukraine (Matrosov, 2013). Eight of the creators were arrested in March 2012, and the ringleader, who was not named, was arrested in April 2013. He was described as a 28-year-old Russian national (Schwartz, 2013).

Carberp runs on all versions of Windows and does not require administrator privileges. One of the characteristics of Carberp is that it is able to evade detection and is able to disable an antivirus program that exists on a host computer. It is also written so that other malware that might exist on the computer will be overridden or erased so Carberp can work unimpeded. This makes the program very difficult to destroy or remove. According to experts, a computer's hard drive must be reformatted to remove the program. If that is not done, the malware will eventually return.

The Carberp Trojan is still available and active. It evolves over time, adding new features as it changes. Some of the changes allow the criminal to have more opportunities to manage the commands over the botnet, a type of computer virus that commands a computer to perform tasks, often without the owner's knowledge. In June 2013, the malware was posted online, making it available to anyone who wants to use it.

The Bolek Trojan, a new banking Trojan, appeared in May 2016. Like Carberp, Bolek is a threat to the financial and banking market. Through use of the Bolek program, criminals are able to steal a victim's login credentials by tracking key strokes and sending information to the offender. Bolek has been known to target Microsoft Internet Explorer, Google Chrome, Opera, and Mozilla Firefox browsers. Bolek can also spread to other files on a computer or network or even spread to other computers.

See also: Malware; Trojan Horse

Further Reading

Krebs, Brian. 2013. "Carberp Code leak stokes copycat fears." Krebs on Security (blog), June 13, 2013. https://krebsonsecurity.com/2013/06/carberp-code-leak-stokes-copycat-fears/

Matrosov, Aleksandr. 2012. "All Carberp botnet organizers arrested." Welivesecurity, July 2, 2012. https://www.welivesecurity.com/2012/07/02/all-carberp-botnet-organizers-arrested/

Matrosov, Aleksandr. 2013. "Carberp: The never ending story." Welivesecurity, March 25, 2013. https://www.welivesecurity.com/2013/03/25/carperb-the-never-ending-story/

Rashid, Fahmida Y. 2011. "Carberp trojan removes antivirus scanners, other malware from host; The latest banking malware Carberp has gone through three versions since it came on the scene last year and continues to add on new features." eWeek.com, January 28, 2011. www.eweek.com/security/carberp-trojan-removes-antivirus-scanners-other-malware-from-host

Schwartz, Matthew J. 2013. "Alleged Carberp botnet ringleader busted." DarkReading, April 5, 2013. https://www.darkreading.com/attacks-and-breaches/alleged-carberp-botnet-ringleader-busted/d/d-id/1109413

CENTER FOR INTERNET SECURITY

The Center for Internet Security (CIS) is a 501(c)(3) nonprofit organization formed in October 2000 to "identify, develop, validate, promote, and sustain best practice solutions for cyber defense and build and lead communities to enable an environment of trust in cyberspace." The CIS is headquartered in East Greenbush, New York, and has corporations, government agencies, and academic institutions as its members. The organization works with these agencies to increase their online security practices.

The organization is part of the Multi-State Information Sharing and Analysis Center (MS-ISAC). This organization works alongside the Office of Cybersecurity and Communications (part of the DHS) to monitor emerging cyber threats and then informs its members (often local and state governments) about those threats. All 50 states are part of MS-ISAC, as are the District of Columbia and territorial and tribal governments. If a threat is credible, they work alongside the government agency to establish efforts aimed at mitigating any possible effects. The mission of the MS-ISAC is "to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery."

Any government agency can become a member of MS-ISAC. It is free for those who work in the federal, state, local, tribal, or territorial government. It is also free for those who work in public K–12 schools and schools of higher education. All members have access to the Security Operations Center, which provides warnings for new attacks or compromises on IP domains. If an attack does occur, the Center provides assistance with incident response and forensics services. They also provide tabletop exercises to help agencies prepare for a possible attack.

Officials at the Center for Internet Security provide tips on how to keep an organization's data secure, such as keeping an inventory of both authorized and unauthorized devices, which can be used to steal data from an organization (or can be lost/stolen themselves). They also suggest controlling administrative privileges (so that fewer people have access to privileged information), establishing malware defenses, and developing methods for data recovery in case data is lost. CIS also provides over 100 guidelines that can be used to safeguard an organization's networks against threats. These consist of best practices that can be used by an organization to assess and improve their computer security. They also provide ways to increase security.

By the end of the third quarter of the 2017 fiscal year, MS-ISAC had identified 97 data breaches, which they identified as being a 141 percent increase as compared to the total number of breaches that were identified in 2016. Given that number, the organization predicted that 2017 would have more data breaches than ever before.

See also: Cybersecurity and Infrastructure Security Agency (CISA)

Further Reading

Center for Internet Security. 2019. https://www.cisecurity.org/cybersecurity-tools/

ISAO Standards Organization. 2018. "Multi-State Information Sharing and Analysis Center (MS-ISAC)." https://www.isao.org/resource-library/other-resources/multi-state-information-sharing-and-analysis-center-ms-isac/

CHANEY, CHRISTOPHER (1977–)

Christopher Chaney was a hacker arrested in 2011 for hacking into the e-mail accounts of numerous Hollywood celebrities, such as Scarlett Johansson, Christina Aguilera, Mila Kunis, and Jennifer Lawrence, among others. In all, Chaney hacked more than 50 e-mail accounts by accessing them through Apple's iCloud for almost a year, beginning in November 2010. Once in the accounts, he sent revealing pictures of the celebrities to another hacker, who then posted the pictures and other information online. The practice of hacking into celebrity accounts is referred to as "hackerazzi." This can be e-mail or social media such as Twitter or Facebook.

Chaney explained that he was able to guess the passwords of the accounts by looking at the celebrities' social media accounts and looking for personal information such as a pet's name, sibling name, or best friend. He spent upward of 20 hours a day looking through social media and other sources of private information on the celebrities. He clicked on the "forgot your password" icon and answered the security questions by using the information he found on other sites. This allowed him to reset passwords and gain access to an account. Chaney then often had access to photographs, calendars, address books, and any other information that was saved there. Some of the information he stole included financial information, personal information, and even a movie script. Chaney could also search the contact list for other e-mail accounts and then tried to break into those. He also changed the accounts so that any e-mails would be automatically forwarded to himself. This meant that if the celebrities became suspicious and changed their passwords, he knew that as well. He was able to have access to some accounts for months without raising any suspicions.

Chaney never sold any of the photos, so he did not profit from his behavior. He saw his hacking as a game—a challenge to see how far he could go. He also wanted to impress other hackers in the hacking community. However, the victims saw his behavior differently. One of his victims, Scarlett Johansson, said that she found Chaney's actions to be "perverted and reprehensible." She said, "As long as he has access to a computer, Christopher Chaney continues to be a threat to women who believe e-mail communications are personal and confidential" (King, 2018, 4). At least one of the victims, 23-year-old actress and singer Renee Olstead, indicated that she considered taking her life after nude photos of her were made public. In addition to hacking into the celebrities' accounts, Chaney also hacked into the accounts of two women he knew personally, sending nude pictures of one of them to her father.

Law enforcement began an inquiry of this and other celebrity hacking events in Operation Hackerazzi. Officials seized the hard drive from Chaney's computer and discovered numerous photos of celebrities along with a document that detailed personal data about each person. Chaney continued to pursue celebrity photos even after the police confiscated his hard drive.

On October 12, 2011, Chaney was arrested and charged with 26 counts of computer hacking, identity theft, and illegal wiretapping. The judge sentenced Chaney to serve 10 years in prison for his offenses and then be placed on three years of supervised probation upon his release. He was also fined $66,179. He could have been sentenced to a maximum of 121 years for those charges.

Upon his arrest, Chaney claimed to be glad he was caught because, as he explained, he was addicted to hacking. His hacking behavior, he said, began as a "curiosity" but quickly turned into an addiction, and he was unable to stop (Zetter, 2011).

See also: Cyberstalking; Hacker and Hacking

Further Reading

King, Robert. 2018. "Lessons from Hollywood cybercrimes: Combatting online predators." *Berkley Journal of Entertainment and Sports Law* 7, 1, pp. 1–12.

McCoy, Terrence. 2014. "Why hackers target celebrities like Jennifer Lawrence—and who they are." *The Washington Post*, September 3, 2014. https://www.washingtonpost.com/news/morning-mix/wp/2014/09/03/why-hackers-target-celebrities-like-jennifer-lawrence-and-who-they-are/?utm_term=.2246f76a8a36

Morse, Andrew. 2011. "Florida man charged in celebrity email-hacking case." *Wall Street Journal*, October 13, 2011. https://www.wsj.com/articles/SB10001424052970204002304576627433276714992

Singer, Bill. 2012. "Hacker of starts gets 10 years in prison." *Forbes*, December 18, 2012. https://www.forbes.com/sites/billsinger/2012/12/18/hacker-of-the-stars-gets-10-years-in-prison/#2bac979f4375

Winton, Richard. 2012. "Scarlett Johansson's celebrity hacker gets 10 year sentence." *Los Angeles Times*, December 17, 2012. http://latimesblogs.latimes.com/lanow/2012/12/hollywood-hacker-scarlett-johansson-sentenced.html

Zetter, Kim. 2011. "Alleged celeb hacker glad he got caught; was addicted to hacking." *Wired*, October 13, 2011. https://www.wired.com/2011/10/hacker-glad-he-got-caught/

CHAOS COMPUTER CLUB

The Chaos Computer Club (CCC) is Europe's largest group of computer hackers. Based in Berlin, Germany, its general mission is to expose flaws in computer security. In addition, the members have other goals. One is to strive for an increased level of transparency in government actions and support a higher level of freedom of information. The members also believe that computers should be more available to the general public. To this end, the members often criticize any legislation that seeks to place limits on the internet. At the same time, the CCC understands that the privacy of those who use the internet must be a top priority.

Computer enthusiasts Wau Holland and Steffen Wenery, from Germany, founded the organization in 1981. Holland proposed that there was a direct link between computers and politics. Holland found himself on the "left" of the political spectrum, with some more radical political thoughts and orientations about government and society. He had the idea that if more people had access to computers, they would be able to liberate themselves from the big businesses that often oppressed citizens. Based on this belief, he deemed his computer hacking should have a political purpose.

The members of the CCC decided that they would hack into different businesses, not only to expose existing security flaws in their computer systems but also to embarrass their political enemies. Immediately after a successful hack, the members would inform law enforcement and the media about their actions. They did this to bring attention to their activities and maximize their actions' impact.

One of the CCC's first successful hacking events, and the first online bank robbery, occurred in 1984 when the group hacked into Deutsche Bundespost, a postal and telecommunications organization in Hamburg, Germany. Prior to the hacking, CCC members informed officials at the company about a system weakness they detected in their computer network, but officials chose to ignore the warnings. In response, CCC members hacked into the system using a password belonging to a savings bank and stole 134,000 Deutsch marks by exploiting security flaws. This allowed the CCC members to transfer a large sum of money into their personal bank accounts. While the members eventually returned all of the money, they were able to expose a major security flaw in the organization that put their customers' financial standing at risk. At the same time, the organization made a major political statement about the lack of government action to increase cybersecurity, and the dangers that could result from that inaction.

Each year, the CCC hosts the Chaos Communication Congress, an annual event that brings together people interested in computer security and privacy issues as well as political issues. The conference has been organized since 1984. Thousands of people attend each year so they can collaborate on projects, listen to speakers, and gain hands-on experience with the newest technology. Each conference has a theme, including "We Come in Peace," "Behind Enemy Lines," "Who Can You Trust?" or "Nothing to Hide!" In 2007, Julian Assange, the founder of WikiLeaks, attended the conference to discuss his WikiLeaks project.

Members of the CCC have sometimes been associated with controversial behaviors. One person who has been affiliated with the group, Karl Koch, allegedly stole secrets and software from the U.S. military and nuclear establishments during the Cold War between the United States and the Soviet Union, and then sold them to the Russian KGB, the government agency responsible for the nation's security at the time. He then sold his story to the media. In May, 1989, his burned body was found by in Germany. Officials labeled his death a suicide, but others are convinced that he was killed in order to prevent him from revealing other secrets.

In 2013, the CCC claimed that they cracked the fingerprint sensor on the Apple iPhone 5S only two days after the product released. They asserted that members of their biometric hacking team lifted a fingerprint of a user from a glass surface and then used that to create a fake fingerprint that was used to unlock a phone. Those responsible used this to point to the dangers of relying on biometrics to control access to technology or data.

The CCC members were also able to hack the iris-recognition element in Samsung's Galaxy S8 smartphone about a month after it was introduced for sale. This time, CCC members used an artificial eye that was made by use of a printer and contact lens. Once again, members sought to highlight the dangers of relying on biometrics as security.

In 2016, members of the CCC demanded an official pardon of Chelsea Manning, who was caught selling classified and sensitive military documents to WikiLeaks. The group made her an honorary member of the CCC.

See also: Anonymous; Assange, Julian; Biometrics; Black-Hat Hackers; Hacker and Hacking; White-Hat Hackers

Further Reading

Arthur, Charles. 2013. "iPhone 5S fingerprint sensor hacked by Germany's Chaos Computer Club." *The Guardian*, September 23, 2013. https://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked

Baich, John. 2008. "The history of the Chaos Computer Club." *Wired*, July 7, 2008. https://www.wired.com/2008/07/the-history-of-3/

Chaos Computer Club. https://www.ccc.de/en/

Hern, Alex. 2017. "Samsung Galaxy S8 iris scanner fooled by German hackers." *The Guardian*, May 23, 2017. https://www.theguardian.com/technology/2017/may/23/samsung-galaxy-s8-iris-scanner-german-hackers-biometric-security

Williams, Elliot. 2018. "Great people and culture at 34th Chaos Communication Congress." Hackaday, January 2, 2018. https://hackaday.com/2018/01/02/34c3-at-last-normal-people/

CHILD PORNOGRAPHY

Federal law in the United States defines child pornography as "any visual depiction of sexually explicit conduct involving a minor." Online child pornography can involve images of children that include explicit sexual acts (as opposed to innocent pictures taken by a parent). The images are used for sexual gratification by the viewer. The meaning or classification of what constitutes child pornography differs between countries and even within countries. It is very much defined by societal mores and values that vary from place to place. In the United States, laws have made it illegal to possess, distribute, or produce internet child pornography. In other countries, it is readily available and easily accessible. For example, a person in Japan is legally permitted to possess the material if they do not have the intent to distribute it. Personal use of child pornography is also legally permitted in Russia, Thailand, and Korea (Akdeniz, 2008).

Laws That Regulate Child Pornography

Most laws pertaining to child pornography describe images of children in sexual poses and acts, but such images may also, in some circumstances, be considered "artistic" works, or even "fantasy." A photo must be sexually suggestive to be considered child pornography. If the images can be categorized as artwork, it may be protected by the U.S. Constitution's First Amendment provisions regarding freedom of expression. However, images of child pornography are not protected by the First Amendment.

By most laws, both the production and consumption of child pornography is illegal. If a person is found to be in possession of child pornography, that person may be labeled as a sex offender by legal authorities and may be forced to register as a sex offender even if there was no physical contact with the victim. An adult who takes a sexually explicit photo of a minor and uploads it to social medial may have committed a federal crime banning child pornography, depending on the circumstances.

There are many federal laws that have provisions to protect children from being sexually exploited and to deter offenders. Some of those include the Protection of Children Against Sexual Exploitation Act (1977), the Child Sexual Abuse and Pornography Act (1986), the Child Protection and Obscenity Enforcement Act (1988), the Child Protection Restoration and Penalties Enforcement Act (1990), and the Child Protection Act (1993).

More recently, two laws have been passed by the U.S. Congress to protect children. The first of these, the Child Pornography Protection Act (1996), banned "virtual" pornography that is created through digital technology and appears to be of a minor, or "conveys the impression that material contains the picture of a child engaged in sexual activities." However, in 2002, the United States Supreme Court struck down the law by ruling in the case *Ashcroft v. Free Speech Coalition* that the provisions of the law were too broad and violated the First Amendment.

Second, Congress passed the Child Obscenity and Pornography Prevention Act (2002). The provisions of this law tries to sidestep the constitutionally treacherous question of virtual child pornography by focusing on the intent of the participants. It outlaws any solicitation to buy or sell child pornography (or anything represented as child pornography).

The Prosecutorial Remedies and Tools against the Exploitation of Children Today Act (PROTECT Act), passed in 2003, was another attempt to deal with virtual child pornography. It would make it illegal to use pornographic images that appear to be indistinguishable from actual children. However, pornographers would be able to defend themselves in court by proving that no actual children were used in making the images, but the burden of proof is essentially shifted from the prosecution to the defense. Another provision would make it illegal to use internet domain names that mislead children into visiting pornographic sites.

Child Pornography on the Internet

Child pornography is big business. Images are publicly available on the internet and often traded and acquired on the dark web. There are thousands of websites that offer images of child pornography. The child pornography industry generates an estimated $3 billion each year (Rogers and Seigfried-Spellar, 2011).

The internet makes the distribution of child pornography easier than in the past. It makes the solicitation of young children by pedophiles almost effortless. The internet allows an offender to have contact with a larger pool of potential victims and does not limit them to a particular geographic area. The victim can be located anywhere around the world. An offender who uses the internet to meet a child is not forced to approach the child in person. Through the internet, the offender is provided with previously nonexistent anonymity that allows them to approach a potential victim more easily and also access images more readily.

An offender may seek to make contact with a young child, which they can do through a chat room or social media site. Once an offender makes contact, they will go through a process of making the victim feel comfortable with the offender in a process called "grooming." An offender will groom a young person for just days or for many months, depending on the child. They may create fake identities and pose a teenagers to befriend a child, usually a vulnerable child who is unhappy or needy. The offender can establish a connection with the child with the long-term intention of sexual abuse or creating a sexual relationship.

Offenders may ask the child to pose for pictures or make pornographic materials and then send the images through the internet. They can also arrange to meet the child to participate in sexual behavior with them. Some offenders are not interested in meeting the children in face-to-face meetings but prefer to remain anonymous and trade images.

The internet also provides offenders with a place to communicate with others who have an interest in child pornography. They are able to "talk" to others and share pictures and tips. When pedophiles find others who are like them, they are likely to view their behaviors as "normal." This may lower inhibitions to act on their impulses (Rogers and Seigfried-Spellar, 2011).

Many experts are also concerned about the availability of online pornographic material to young people. It is estimated that about 90 percent of minors aged 8–16 have viewed pornography online, with the average age of first exposure being around 11 years old (Rogers and Seigfried-Spellar, 2011).

In some states in the United States, officials have started to charge minors with committing criminal offenses if they send or post nude photos of themselves (selfies) on the internet, even if they do so willingly. Some have been prosecuted under child pornography statutes. This means that a high school student who decides to send a selfie that is sexual in nature to their significant other could be charged with violating laws related to child pornography.

Additionally, the person who received the picture may also be charged. If the photo is shared with other people, those who receive it could also be charged. Many states are bringing these charges for many reasons, one of which is to protect the child from those images having a permanent presence on the internet. On a broader scale, deterring the posting of nude pictures is also an attempt to reduce the amount of child pornography available on the internet for others to view or even manipulate.

Combating Pedophile Information Networks in Europe

The University College Cork in Cork, Ireland, founded the Combating Pedophile Information Networks in Europe (COPINE), housed within the Department of

Applied Psychology in 1997. The analysts gathered over 80,000 images of children in sexual situations that were readily available on the internet. After reviewing the images for the severity of abuse in the images, they created a typology of 10 levels of severity. One of the findings was that the age of the children involved in child pornography was become younger over time. This raised the concern that, because the children are so young, they are not able to express to others what is happening to them or even understand that what they are experiencing is wrong. The researchers also found an increase in pictures that seemed to be created in a family setting, such as in a family room located in a home or even where the offender is a family member. They termed this "domestic" pornography.

Another finding from COPINE was that over half of the victims in the pornographic images depicted young women, but there was a trend toward more young men in the images. Finally, they noted changes over time in the racial makeup of the pictures. Specifically, white children were more likely to be the subject of pictures that depict violent acts, whereas Asian children were more likely to be in posed pictures. Overall, there were few children of African-American descent in any of the images (Jewkes and Andrews, 2007).

In 2005, research about child pornography through this organization was transferred to INTERPOL, the International Police Organization, which represents 194 countries. This allows for a more extensive collection of information about child pornography.

Law Enforcement's Battle against Child Pornography

Most law enforcement agencies on the state and local levels have specialized units or task forces that are responsible for investigating allegations surrounding the use of technology to harm children. In order to locate offenders, police officers often go to online chat rooms or social media sites and pretend to be minors in sting operations. They may agree to meet the offender in a real location, where the offender is arrested or taken into custody. This technique requires police officers to have a certain level of competence with technology.

Law enforcement officials face other obstacles when investigating online child pornography. One is the question of jurisdiction. While the materials are available online, the sites may be hosted in another country where the officers are not permitted to act. Because of jurisdictional limitations, law enforcement may be aware of offenders but unable to act. In some areas, there may be a limited number of laws that give law enforcement the authority to arrest an offender. In some places, social and cultural norms may be more permissive of child pornography, and the legal definitions of offenses may not encourage law enforcement to crack down.

Beyond this, some departments may not have financial resources to fight child pornography to the extent they may want. Because such a huge volume of pornography is available online, it becomes an almost impossible task to eliminate it or even limit its availability.

See also: Dark Web

Further Reading

Akdeniz, Yaman. 2008. *Internet child pornography and the law: National and international responses*. Burlington, VT: Ashgate Publishing.

Casey, Eoghan. 2004. *Digital evidence and computer crime*. Boston, MA: Elsevier.

Jewkes, Yvonne, and Carol Andrews. 2007. "Internet child pornography: International responses." In *Crime online*, edited by Yvonne Jewkes, 60–80. Devon, UK: Willan Publishing.

Rogers, Marcus K. and Kathryn C. Seigfried-Spellar. 2011. "Internet child pornography: Legal issues and investigative tactics." In *Crime on-line*, edited by Thomas J. Holt, pp. 113–144.

Wolak, J., D. Finkelhor, and K. J. Mitchell. 2005. *Child pornography possessors arrested in internet-related crimes: Findings from the National Juvenile Online Victimization Study*. Washington, D.C.: Center for Missing and Exploited Children.

CHINA

Cybercrime is a problem in China just as it is in the United States. In 2011, roughly 100,000 cases of online and telephone fraud occurred in China, according to the Chinese Ministry of Public Security. The number of fraud cases increased to 400,000 in 2014 (Tatlow and Boehler, 2015). In 2016, the Beijing Public Security Bureau received over 20,000 complaints of online fraud victimization. The amount lost by victims in those incidents was over $28 million. Though the number of complaints received was lower than the previous year, the average amount of monetary loss suffered by victims increased (Cheng, 2017). Some of the schemes perpetrated by cybercriminals include the use of fraudulent website to sell nonexistent tickets to events, fraudulent employment schemes where victims are persuaded to buy items for the cybercriminals as part of the job application process, and posing as government officials to extort money from victims over legal issues fabricated by the cybercriminal (Cheng, 2017; Tatlow and Boehler, 2015). Victims of online fraud in China tend to live in provinces that are more economically developed (Cheng, 2017). Commission of cybercrime in China can result in prison time for the perpetrators. However, it appears as though probation may be a more common punishment. The average amount of prison time that convicted cybercriminals receive appears to be decreasing. In 2012, the average term of incarceration for a convicted cybercriminal was 45 months. In 2016, the average dropped to 28 months (Stilgherrian, 2017). As with other countries, the cybercriminals committing crime in China are not necessarily in China themselves, making apprehension difficult. Among those cybercriminals are Chinese expatriates (Cheng, 2017).

There are certain activities in China that would be considered a cybercrime that would not be considered a cybercrime in the United States. These offenses stem from China's laws regarding permissible content on the internet. China's system of censorship is the largest in the world, blocking websites such as Google, Facebook, and the *New York Times* (Bloomberg News, 2018). This censorship apparatus has been dubbed "The Great Firewall of China." The United States does legally prohibit certain online material, such as child pornography. Accessing that material could result in criminal charges. In China, the scope of prohibited online activities is wider, and it appears to have political motivations. In 2001, two Chinese journalists were arrested for posting writings online that were in favor of democracy and deemed subversive by the Chinese government. The journalists were each sentenced to 10 years of prison (Cohn, 2007). A crackdown on similar behavior occurred in 2013. The Chinese government targeted Chinese bloggers who posted writings that were critical of the Chinese government, claiming those bloggers were spreading false information. Hundreds of bloggers were arrested on these charges (Buckley, 2013). Similar arrests of Chinese citizens were made in 2017 for posting material deemed subversive or otherwise objectionable by the Chinese government. In some of those instances, the things written were written in private communications (Bloomberg News, 2018).

Chinese cybercriminals commit crimes against international victims as well. This is perhaps most prevalent in the area of intellectual property theft. China is the world leader in intellectual property right infringement. China accomplishes this theft through both physical and cyber methods. In 2015, 87 percent of the all counterfeit goods that were seized at the United States border were from China (including Hong Kong). That same year, 61 percent of the software in use in Asia in general was pirated (Commission on the Theft of American Intellectual Property, 2017).

The Chinese government itself has been involved—directly or tacitly—in the commission of cybercrimes. Indeed, China is the most prolific offender when it comes to cyberattacks. From 2006 to early 2019, China perpetrated over 100 cyberattacks on different countries—the most of any country in that time span. The countries attacked by China in that time frame include the United States, France, the United Kingdom, South Korea, Canada, India, and Belgium (Center for Strategic and International Studies, 2019). It appears that a significant portion of the cyberattacks carried out by China are focused on governmental and business espionage. In 2009, Canadian officials indicated they found evidence of a governmental espionage system installed on the computer networks of over 100 countries, and that they believed China was behind that espionage. In 2010, Google announced that it and over 30 other companies had their networks attacked by China, part of their intent being to collect technological information (Center for Strategic and International Studies, 2019).

Evidence of how China engaged in some espionage efforts emerged in 2015. The evidence was discovered as part of an investigation that Amazon was conducting into the servers of Elemental Technologies—a business it was considering acquiring. In the course of that investigation, it was found that microchips were installed in the servers that were not included in the schematics for those servers. The motherboards were manufactured in China. It is believed that the People's Liberation Army (the Chinese military) installed these microchips during the manufacture of the motherboards in China, and that the chips allowed China to monitor the activity of the servers in which the chips were installed. The servers that Amazon investigated were also used by various government agencies and large corporations (Robertson and Riley, 2018). Additional possible instances of governmental espionage by China have arisen since that time. In 2017, China Aerospace Science and Industry Corporation—a state-owned corporation—allegedly sold biometric hardware to Taiwan that included undisclosed backdoors that China could exploit to track who was leaving and entering Taiwan. In 2018, China allegedly installed spyware on the computer network it provided to the African Union—a claim that China denied (Center for Strategic and International Studies, 2019).

It appears that China has also been active in business espionage since that time. China has policies in place that emphasize the acquisition of foreign intellectual property, such as technology. These policies often act to put Chinese entities in an advantageous position to steal intellectual property from foreign businesses operating in China (Commission on the Theft of American Intellectual Property, 2017). Efforts to steal foreign technological intellectual property appear to be ongoing as well. In 2018, the United States, Australia, Canada, New Zealand, and the United Kingdom accused China of conducting cyberespionage operations that targeted intellectual property of companies in twelve different countries. This operation had been carried out over twelve years (Center for Strategic and International Studies, 2019). It appears that the companies most vulnerable to these cyber espionage attacks from China are technology companies that are at the forefront of technological advancement (Commission on the Theft of American Intellectual Property, 2017). Chinese cyberattacks are not necessarily sophisticated. James Comey, former director of the FBI, said this about cyberattacks from the Chinese:

> I liken them a bit to a drunk burglar. They're kicking in the front door, knocking over the vase, while they're walking out with your television set. They're just prolific. Their strategy seems to be: "We'll just be everywhere all the time. And there's no way they can stop us." (Osborne, 2014)

China has been on the receiving end of cyberattacks as well. From 2006 to early 2019, China was the victim of approximately 25 cyberattacks (Center for Strategic and International Studies, 2019). In 2011, China created a cyber defense squad within the People's Liberation Army to protect against cyberattacks (Beech, 2011). There has been some indication that China is moving toward more firm regulation of cybercrime, both domestically and internationally. In 2016, Meng Hongwei was appointed president of Interpol, an international law enforcement organization. Meng Hongwei was also the deputy head of the Ministry of Public Security in China. In his capacity as president of Interpol, Meng expressed the need for international cooperation in combating cybercrime, noting that individual countries would not be able to address cybercrime alone (Meng, 2017). Meng's speech was seen by some as an indication that China was moving toward more comprehensive regulation of cybercrime (Waterman, 2017). However, Meng was arrested by China in 2018 for bribery. There is some speculation that the arrest was made for political purposes. In a statement made by China's Ministry of Public Security, it was said that Meng's "insistence on doing things in his own way" was why he was under investigation (Chi-yuk and Ho, 2018). It has been suggested that this focus on Meng's individual willfulness may be an indication that Meng did not adhere to Communist Party lines, which may have landed him in trouble (Chi-yuk and

Ho, 2018). Meng's wife believes her husband's arrest was spurred on by rivals in the Ministry of Public Security (Graham-Harrison, 2018). Whatever the exact reason, it is now unclear whether Meng's statements reflect the intentions of China is regards to a unified effort to combat cybercrime internationally.

See also: Biometrics; Copyright Infringement; Federal Bureau of Investigation; Firewall; International Issues; People's Liberation Army Unit 61398; Political Uses; Spyware

Further Reading

Beech, Hannah. 2011. "Meet China's newest soldiers: An online blue army." *Time*, May 27, 2011. http://world.time.com/2011/05/27/meet-chinas-newest-soldiers-an-online-blue-army/

Bloomberg News. 2018. "The great firewall of China." *Washington Post*, November 5, 2018. https://www.washingtonpost.com/business/the-great-firewall-of-china/2018/11/05/5dc0f85a-e16d-11e8-ba30-a7ded04d8fac_story.html?utm_term=.a3cc398e98bd

Buckley, Chris. 2013. "Crackdown on bloggers is mounted by China." *New York Times*, September 10, 2013. https://www.nytimes.com/2013/09/11/world/asia/china-cracks-down-on-online-opinion-makers.html?pagewanted=2&_r=0&hp

Center for Strategic and International Studies. 2019. "Significant cyber incidents." Center for Strategic and International Studies. https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

Cheng, Ron. 2017. "Cybercrime in China: Online fraud." *Forbes*, March 28, 2017. https://www.forbes.com/sites/roncheng/2017/03/28/cybercrime-in-china-online-fraud/#46db663f7ac3

Chi-yuk, Choi, and Matt Ho. 2018. "China accuses former Interpol chief Meng Hongwei of taking bribes." *South China Morning Post*, October 8, 2018. https://www.scmp.com/news/china/politics/article/2167451/china-accuses-former-interpol-chief-meng-hongwei-taking-bribes

Cohn, William A. 2007. "Yahoo's China defense." *New Presence: The Prague Journal of Central European Affairs* 9, 3, pp. 30–33.

Commission on the Theft of American Intellectual Property. 2017. "Update to the IP Commission Report." http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf

Graham-Harrison, Emma. 2018. "'It's not justice': Wife of detained Interpol chief faces down China." *The Guardian*, November 18, 2018. https://www.theguardian.com/world/2018/nov/18/wife-detained-interpol-chief-faces-down-china-grace-meng-hongwei

Meng Hongwei. 2017. "To ride the tide of the times and keep the hopes of a century: An Interpol that faces the future." Interpol, September 26, 2017. https://www.interpol.int/content/download/5351/file/Speech%20by%20President%20Meng%20Hongwei%2086GA.pdf

Osborne, Charlie. 2014. "FBI chief compares Chinese hackers to 'drunk burglars.'" ZDNet, October 6, 2014. https://www.zdnet.com/article/fbi-chief-compares-chinese-hackers-to-drunk-burglars/

Robertson, Jordan and Michael Riley. 2018. "The big hack: How China used a tiny chip to infiltrate U.S. companies." *Bloomberg Businessweek*, October 4, 2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Stilgherrian. 2017. "Cybercrime in China is the same, but different." *ZDNet*, August 10, 2017. https://www.zdnet.com/article/cybercrime-in-china-is-the-same-but-different/

Tatlow, Didi Kirsten, and Patrick Boehler. 2015. "Online and telephone fraud surges in mainland China and Hong Kong, officials say." *New York Times*, August 18, 2015. https://sinosphere.blogs.nytimes.com/2015/08/18/online-and-telephone-fraud-surges-in-mainland-china-and-hong-kong-officials-say/?_r=0

Waterman, Shaun. 2017. "How an Interpol speech shows that China may be evolving on cybercrime." *Cyberscoop*, July 7, 2017. https://www.cyberscoop.com/china-cybercrime-meng-hongwei-interpol/

CLEARY, RYAN (1992–)

Ryan Cleary, also known as ViraL, was a member of LulzSec, a computer hacking group. When Cleary was 19, he was arrested for carrying out cyberattacks in London and the United States. Officials also charged him with creating a botnet that allowed him to direct the attacks. Cleary was arrested in 2012 along with fellow hacker Jake Davis, who was also 19.

A Wickford, Essex, England, native, Cleary admitted to hacking into the Central Intelligence Agency (CIA), the Pentagon, Sony, Nintendo, the Arizona State Police, Westboro Baptist Church, PBS, 20th Century Fox, and the Serious Organised Crime Squad in England by using DDoS attacks that overwhelm websites, causing them to shut down. He uploaded personal information of hundreds of thousands of people to the internet, including hundreds of sensitive internal documents concerning border operations from the Arizona Department of Public Safety.

Cleary was charged with violating the British Criminal Law Act and Computer Misuse Act. Specifically, he was charged with one count of conspiracy to contravene the provisions of the Computer Misuse Act of 1990, three charges related to the intent to commit an unauthorized act under the Computer Misuse Act 1990 and one count of making, supplying or obtaining articles for use in an offense under the Computer Misuse Act of 1990.

In the ensuing investigation that was carried out jointly by the British Metropolitan Police Department and agents from the FBI, officials discovered 172 images of child pornography on his computer that depicted infants as young as six months. He pleaded guilty to two counts of making indecent images and one count of possessing indecent images.

In 2013, Cleary was sentenced to prison for two years and eight months for the hacking offenses and then to a period of community service for the pornography. He could have received a sentence of up to 10 years upon conviction.

See also: Bots and Botnets; Distributed Denial-of-Service Attack (DDoS); LulzSec

Further Reading

Dodd, Vikram, and Josh Halliday. 2011. "Teenager Ryan cleary charged over LulzSec hacking." *The Guardian*, June 22, 2011. https://www.theguardian.com/technology/2011/jun/22/ryan-cleary-charged-lulzsec-hacking

Greenwood, Chris. 2013. "Lulzsec hacker caught with child porn." *The Daily Mail*, June 12, 2013. www.dailymail.co.uk/news/article-2340144/LulzSec-hacker-caught-child-porn-images-freed-immediately-judge-rules-spent-time-prison-cyber-attacks.html

Leyden, John. 2013. "Jailed LulzSec hacker cleary coughs to child porn images, will be freed soon." *The Register*, June 12, 2013. https://www.theregister.co.uk/2013/06/12/cleary_lulzsec/

Somaiya, Ravi, and Steve Lohr. 2011. "British police charge teenager in connection with hacking attacks." *New York Times*, June 24, 2011. https://www.nytimes.com/2011/06/24/technology/24hack.html

CODE RED

Code Red was a computer worm, a form of malware, that appeared in computers around the world in July 2001. It affected computers using Microsoft's Windows 2000 and Windows NT operating systems. It was named "Code Red" after a kind of Mountain Dew that two employees of eEye Digital Security were drinking as they attempted to analyze the worm and disassemble it.

Code Red was a self-replicating malicious code that sought out a possible vulnerability in a computer and then exploited it. Once it was able to infect a system, the worm multiplied and scanned random IP addresses to find other vulnerable servers. The worm was programmed to deface the home page of the infected computers and launch a DoS attack.

When Code Red infected a machine, it showed a message that read "Hacked by Chinese." During the first 19 days after a computer was infected, the worm spread itself to other computers. During days 20–27, the worm began a DoS attack on several IP addresses, including the White House. This meant that all of the infected computers contacted the White House website at the same time, overloading the networks. On day 28 and after, the worm initiated no attacks as the computer was put into a state of permanent sleep.

In addition to this, the worm established a backdoor into the operating system of the computer. This permitted a remote user to have access to the machine and control it. The person would then have access to the victim's computer and all of the data stored on it.

When the worm was most active, over 2,000 computers were infected per minute. The worm was estimated to affect 300,000 servers in 14 hours, about half the number of servers in the United States. Although the effects of Code Red did not last long, it is thought that about six million servers around the world had to be checked for the worm and then have a patch applied to close the security hole that was originally exploited by Code Red, costing an estimated $10 billion.

Code Red Version 2 emerged in computer systems in July 2001. The worm infected DSL modems, printers, and routers. This worm randomly found vulnerable computers that happened to be on the same computer network as the infected machine and spread the worm to the other machines. The worm could determine if the language system was set to Chinese. If it was not, then the worm would continue to spread for 24 hours. It was estimated that more than 359,000 computers were infected within 14 hours after it was released. It was designed to stop spreading on October 1. The second Code Red worm caused more damage than the first, largely because there were more machines infected. The worm gave hackers the ability to steal sensitive information like passwords or credit card numbers from the infected machines.

Microsoft sent out a patch to users that they could download to protect their computers from the Code Red II worm, but it was sent five weeks before the virus became well known. This meant that many people did not recognize the urgency and did not apply the patch (Sans Institute, 2001a). Many were able to install some antivirus software before Code Red 2 was released. Most people were able to remove the first wave of Code Red by rebooting the system, which removed the worm from the computer's memory, but removing the second Code Red was much more difficult. The second worm was written to be much more covert, making it more difficult to detect and to remove. Those computers infected with Code Red 2 had to be reformatted, which would erase the entire malware program as well as the backdoor.

The creator of the Code Red worm is not known. Many believed it to be the product of Chinese hackers. Others believed the worm had its origins in hackers at the DEF CON convention that year. Most people agreed that it was a well-written, complex worm, so the author had to be someone with a background in computers. In the end, it was estimated that the cost of the Code Red virus was $2.6 billion, and losses in productivity amounted to $1.5 billion.

See also: DEF CON; Morris, Robert Tappan; Nimda; Worm

Further Reading

Meinel, Carolyn. 2002. "Code Red: Worm assault on the Web." *Scientific American*, October 28, 2002. https://www.scientificamerican.com/article/code-red-worm-assault-on/

Sans Institute. 2001a. "The mechanisms and effects of the Code Red worm." https://www.sans.org/reading-room/whitepapers/dlp/mechanisms-effects-code-red-worm-87

Sans Institute. 2001b. "What is Code Red worm?" https://www.sans.org/reading-room/whitepapers/malicious/code-red-worm-85

Stenger, Richard. 2001. "New 'Code Red' worm entices web hijackers." CNN, August 7, 2001. www.cnn.com/2001/TECH/internet/08/06/code.red.two/index.html

Wong, Nicole C. 2001. "'Code Red' creeping worldwide." *The Washington Post*, August 2, 2001. http://www.washingtonpost.com/wp-dyn/articles/A20063-2001Aug1.html

COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE

The Comprehensive National Cybersecurity Initiative is a plan to strengthen the U.S. response to cyber incidents. The plan was launched by President George W. Bush in the National Security Presidential Directive 54/Homeland Security Presidential Directive 23 that was announced in January 2008. These documents were intended to improve the nation's cybersecurity against cyberthreats.

In 2015, President Obama described the "serious risks to national and economic security from malicious cyber activity" (Obama, 2015). He ordered a review of the existing federal policies for cybersecurity with regards to protecting the nation's infrastructure. He asked for a comprehensive plan to increase the nation's cybersecurity. To do this, he created the Cyberspace Policy Review Committee, which was to perform a 60-day review of the country's cybersecurity policies. They were given instructions to work closely with all critical players in state and local governments, including the private sector, to develop a new, more comprehensive plan for U.S. cybersecurity. He made it clear that the plan needed to protect individual rights and civil liberties of all people.

There were three goals identified by the Committee. They included:

1. To establish a front line of defense against today's immediate threats
2. To defend against the full spectrum of threats
3. To strengthen the future cybersecurity environment

The plan that emerged is the Comprehensive National Cybersecurity Initiative. The plan revolved around 12 initiatives:

1. Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections: The Trusted Internet Connections is a plan to consolidate the external access points to the Internet. This will result in increased security.
2. Deploy an intrusion detection system of sensors across the Federal enterprise: This will help to identify an unauthorized user if they attempt to gain access to a federal computer network. This is part of Einstein 2, a program used by the U.S. federal government that monitors computer traffic and is used to detect malicious activity.
3. Pursue deployment of systems to prevent intrusion across Federal agencies: Einstein will be used to identify malicious programs as a way to increase the security of networks. It can detected cyber threats and respond to them before they cause harm.
4. Coordinate and redirect efforts for research and development: It is hoped that this will allow for more coordination of research activities to reduce redundancies in research efforts, making for more cost-efficient research.
5. Connect cyber-ops centers as a way to increase communication: By promoting interagency collaboration, centers can easily share data on possible malicious activities directed toward federal agencies and stop an attack before it is launched.
6. Develop and carry out a governmentwide cyber-counterintelligence plan: A plan is needed to coordinate all activities carried out by federal agencies as they attempt to detect, deter and mitigate cyber threats to the United States. This needs to include increased cyberintelligence education and awareness plans.

7. Increase the security of classified networks. These networks hold highly sensitive information on diplomatic issues, law enforcement cases, homeland security operations, and other critical concerns. These need to be protected from successful penetration by cybercriminals.
8. Expand cybereducation: It is essential to give people the knowledge and skills to carry out the new technology to prevent cybercrimes from occurring. There is a demand for cybersecurity experts to teach these skills as existing programs lack unity and focus. The country needs to develop a workforce that is technologically skilled and cyber-savvy.
9. Define and develop "leap-ahead" technology and programs: It is important to develop cybersecurity technology that is beyond current systems. This way, it can be deployed 5 to 10 years in the future.
10. Define and develop enduring deterrence strategies and programs: Planners must consider long-range solutions for cybersecurity, not simply traditional approaches.
11. Develop a multipronged approach for global supply chain risk management: Cybercriminals have increased opportunities for harming the United States by affecting the supply chain as a way to gain unauthorized access to data. New policies must reflect the global marketplace and complex relationships that now exist.
12. Define the federal role in extending cybersecurity into critical infrastructure domains: Many critical infrastructure are operated by private individuals who rely on efficient operation of systems that are vulnerable to cyberattacks. There must be an ongoing relationship between the federal government and the operators of critical infrastructure to share information and prevent crime.

The Utah Data Center, a shorter name for the Intelligence Community Comprehensive National Cybersecurity Initiative Data Center, was built to support the Comprehensive National Cybersecurity Initiative. The Center, completed in 2014, serves as a storage facility for data collected under the initiative, including information on e-mails, phone calls, and data related to internet searches by U.S. citizens, among other things. The facility is a highly secure complex that is geared toward providing technical assistance to employees in the Department of Homeland Security (DHS). They are also responsible for gathering intelligence pertaining to cyberthreats.

The NSA is responsible for overseeing the data collection and storage there. This has been considered controversial by those who claim that the NSA has data-mined individuals' online behaviors and "overcollected" personal information. They point out that data collection and surveillance of individuals became easier after the 9/11 terrorist attacks, which, some people argue, has been unconstitutional and illegal. On the other hand, supporters argue that the data collection can help to prevent future acts of terrorism, including cybercrimes.

See also: Cybersecurity; Data Sovereignty; Einstein; President and Cybercrime

Further Reading

Cyberspace Policy Review. 2009. https://epic.org/privacy/cybersecurity/Cyberspace_Policy_Review_final.pdf

Burrington, Ingrid. 2015. "A visit to the NSA's data center in Utah." *The Atlantic*, November 19, 2015. https://www.theatlantic.com/technology/archive/2015/11/a-visit-to-the-nsas-data-center-in-utah/416691/

Bush, George W. 2008. "National Security Presidential Directive 54/Homeland Security Presidential Directive/HSPD-2." January 8, 2008. https://fas.org/irp/offdocs/nspd/nspd-54.pdf

Obama, Barack. 2015. "Joint statement by President Obama and Prime Minister Narendra Modi of India—Shared effort, progress for all." The American Presidency Project, January 25, 2015. https://www.presidency.ucsb.edu/node/309229

Rollins, John and Henning, Anna C. 2009. *Comprehensive national cybersecurity initiative: Legal authorities and policy considerations*. Washington, D.C.: Congressional Research Service.

White House. n.d. "Foreign policy: The comprehensive national cybersecurity initiative." https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative

COMPUTER FRAUD AND ABUSE ACT OF 1986

In 1986, Congress amended the Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030), originally passed in 1984, making it the primary federal-level statute on computer crime, particularly for hacking-related offenses. The new law prohibits the selling or renting of malware programs that allows an offender to gain access into other systems. It also criminalizes trafficking in passwords for those computers that are identified as "protected computers." If an offender chooses to carry out an attack on another computer and causes significant damage, they can be criminally prosecuted. In general, the legislation aimed to deter malicious hacking and unauthorized access to computer systems. The law was written to protect national security, financial and commercial information, medical records, and interstate communication against mischievous attacks.

In the mid-1970s, as computers and the internet were developing and becoming more widely used, members of Congress first began to recognize the potential for criminal acts committed through this new medium. In 1977, some members of Congress proposed the Federal Computer Systems Protection Act, one of the first bills proposed in Congress to create new laws on cybercrime. This bill did not have enough support by the members and did not pass.

By the mid-1980s, the threat of cybercrime was more obvious, and Congress garnered enough support to pass legislation on cybercrime. In 1984, they passed the Counterfeit Access Device Act as well as the Computer Fraud and Abuse Act. These laws were very narrow scope and lacked detail and clarity, leaving many people confused. In an effort to pass a more useful law, Congress amended the original Computer Fraud and Abuse Act in 1986. The original bill was then amended in 1989, 1994, 1996, and 2001 (in the USA PATRIOT Act), 2002, and then again in 2008.

The updated version of the Computer Fraud and Abuse Act remains the primary federal-level statute on computer crime in the United States. The law bans the dissemination of malware and the trafficking in computer passwords for "protected computers." According to the legislation, a "protected computer" is one that is used by a financial institution or by employees of the U.S. government. It can also refer to computers that are used in interstate or foreign commerce.

Under the law, if a person is able to access restricted information by hacking into a computer, by otherwise accessing a computer without authorization, or by exceeding their authorized access, and that information could be used to injure the United States, or if it communicated or delivered to a person not authorized to receive it, they may be guilty of a felony criminal offense. In short, if a person gathers restricted information without permission, or exceeds granted authorization, and then uses that information in a way that can harm the United States, they have committed a criminal offense.

In other provisions, the law bans the use of DoS attacks that cause a loss of $1,000 or more to a business or agency, called a malicious damage violation. A person can also be convicted if they damage a computer or information, traffic or sell passwords, or threaten to damage a protected computer.

Importantly, the CFAA allows for civil remedies so that a person who suffers a loss as the result of hacking or a DoS attack will be able to bring a civil action against the offender as a way to receive compensation.

The first person to be criminally charged under the law was Robert Morris Jr., a graduate student at Cornell University who, in 1988, released the Morris worm into cyberspace. The malware replicated itself in networks more quickly than he had anticipated, causing many machines around the country to crash. The worm caused a great deal of damage to computers. Morris was convicted in December 1990 for unauthorized access to federal computers and for causing damage.

About the same time (in 1988), Robert Riggs obtained unauthorized access to Bell South's computer system and downloaded information regarding an enhanced 911 system for emergency services. Riggs then sent the information to Craig Neidorf, who in turn published it in a newsletter called *Phrack*, a magazine read by computer hackers. In 1990, both Riggs and Neidorf were charged under the CFAA. Riggs was eventually convicted criminally for hacking into Bell South, and the charges against Neidorf were dropped after the trial judge declared a mistrial.

The CFAA was also used to charge Lori Drew, a 49-year-old woman who in 2006 created a fake MySpace account as a way to cyberbully her daughter's friend, 13-year-old Megan Meier. Drew pretended to be a young male and established a friendship with Megan. After months of sending positive messages, Drew began to send hurtful messages that said, "You are a bad person and everybody hates you. . . .The world would be a better place without you" (Wolff, 2016). Megan took her own life due to the harassment. Prosecutors charged Drew under the CFAA as having "unauthorized access" to MySpace's computers.

Prosecutors relied on the CFAA to charge members of the hacking group Anonymous with crimes after they disrupted the PayPal website in 2010. Officials charged one member, Aaron Swartz, with 11 crimes, as defined by the CFAA, after he used a laptop issued by the Massachusetts Institute of Technology to download millions of scholarly articles from JSTOR. After the charges were filed against Swartz, he took his own life.

The law has been amended multiple times since the original law was passed. In 1994, new amendments allowed victims of computer hacking crimes to bring civil actions as well as criminal charges against an offender. This means that a victim of a computer crime is able to sue an offender for any damage to a computer that results from the unauthorized access. This provision is used frequently by businesses against employees who steal secrets. Another amendment in 1996 changed the law to replace "federal interest computer" with "protected computer."

More extensive changes were made in 2001 in the USA PATRIOT Act. One of those changes defined more clearly what was meant by "loss." This was defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." This can include things such as lost employee wages, lost sales, or other costs incurred because of the crime.

In 2013, after Swartz's death, members of Congress proposed Aaron's Law, a bipartisan proposal to further amend the original CFAA (HR 2454). The new provisions were introduced by Representatives Zoe Lofgren (D-CA) and Jim Sensenbrenner (R-WI) and Senator Ron Wyden (D-Oregon). They made the proposal after complaints that the law was too ambiguous when it came to the definition of "without authorization." Additionally, the law did not define "exceeds authorized access." Aaron's Law removed provisions that made breaches of terms of service and user agreements from the law. It also defined "unauthorized access" to be "circumventing one or more technological measures that exclude or prevent unauthorized individuals from obtaining or altering" information on a protected computer. Despite the bipartisan support, Aaron's Law did not have enough support to pass.

There are six sections to the CFAA. In Section 1, activities that are used by a hacker to gain unauthorized access to information on national defense, foreign relations, and atomic energy are criminalized. If found guilty of these acts, an offender could be sentenced to a fine and/or up to 10 years imprisonment if it were a first offense, or incarceration of up to 20 years for subsequent offenses. Section 2 focuses on hacking of records held by a financial institution, credit card issuer, or consumer-reporting agency. Offenders found guilty of these offenses could be sentenced to a monetary fine and and/or up to one year in prison for a first offense. If the offense was reoccurring, the offender could be sentenced to term in prison of up to 10 years.

Section 3 bans any interference with government operations by obtaining unauthorized access to government-owned computers or computers that are used by government officials. The penalties set by Congress for violation of this included a monetary fine with a possible prison term of up to one year for a first offense, or up to 10 years for subsequent offenses. More offenses were described in Section

4. Here, Congress focused on hacking in which offenders are able to obtain unauthorized access to a federal interest computer to commit fraud or theft. These offenses could be punished by a fine and/or up to five years imprisonment for a first offense, or a maximum of 10 years in prison for subsequent offenses.

There are two parts to Section 5. In the first one, Congress wrote "Whoever . . . through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command to a computer or computer system if the person causing the transmission intends that such a transmission will damage, or cause damage to, a computer, computer system, network, information, data, or program; or withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data, or program," provided the access is unauthorized and causes loss or damage of $1,000 or more over a one-year period or "modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals." A person convicted under this portion of the statute faced a possible fine and/or up to five years imprisonment for a first offense and up to 10 years for subsequent offenses. In the second part, the law defined it a crime for a person who, "…through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command to a computer or computer system with reckless disregard of a substantial and unjustifiable risk that the transmission will damage, or cause damage to, a computer, computer system, network, information, data, or program; or withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data or program" provided the access is unauthorized and causes loss or damage of $1,000 or more over a one year period or "modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals." A person found guilty of this could be sentenced to a fine and/or up to one year in prison.

Finally, Section 6 made it a crime to traffic in passwords that affect interstate commerce or involve the password of a computer that is used by or for the U.S. government. The penalty associated with this offense was defined as a fine and/or up to one year imprisonment for a first offense and up to 10 years for subsequent offenses (Casey, 2004, p. 64).

The CFAA has been criticized over the years for being poorly written and unclear. Many point to the lack of definition of key terms including "unauthorized." Under the law, a person can be prosecuted for violating the "terms of service" policies that are found on almost every piece of software that users upload onto their computers. Prosecutors who charge offenders with crimes based on this law are sometimes criticized because of these possible flaws.

See also: Anonymous; Cyberbullying; 414s; Morris, Robert Tappan; Swartz, Aaron; Worm

Further Reading

Casey, Eoghan. 2004. *Digital evidence and computer crime*. Boston, MA: Elsevier.

Kerr, Orin S. 2010. "Vagueness challenges to the Computer Fraud and Abuse Act." *Minnesota Law Review* 5, pp. 1561–1587.

Wolff, Josephine. 2016. "The hacking law that can't hack it." *Slate Magazine*, September 27, 2016. http://www.slate.com/articles/technology/future_tense/2016/09/the_computer_fraud_and_abuse_act_turns_30_years_old.html

Wu, Tim. 2013. "Fixing the worst law in technology." *The New Yorker*, March 18, 2013. http://www.newyorker.com/news-desk/fixing-the-worst-law-in-technology

CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM)

Continuous Diagnostics and Mitigation (CDM) is a program created by Congress to increase the security of the computer networks and systems belonging to agencies and departments of the U.S. federal government. The CDM program provides federal agencies with the means to identify cybersecurity risks on an ongoing basis; to prioritize those security risks based on the severity of the potential impacts; and then assist cybersecurity personnel in those agencies to mitigate the most significant problems first, then follow through with secondary problems. The program is overseen and implemented by the U.S. DHS. CDM is part of the federal government's ongoing efforts to protect the government's computer systems by providing federal agencies with additional training, knowledge, and tools needed to identify possible cybersecurity risks and then mitigate problems. In short, it is a way to strengthen the cybersecurity of the federal government.

The key objectives of the program are to reduce the threats to agencies, streamline reporting of potential threats, and improve the response capabilities of the federal government. Phase1 of the program, called "What Is on the Network," requires the management and control of devices and software linked to a computer network. Phase 2 is entitled "Who Is on the Network." The goal of this phase is to collect data on every user who is connected to an agency's network, which will provide an overall view of the entire user population. Phase 3, or "What Is Happening on the Network," looks at data that is being sent into and out of the agency, as well as user behavior and activities. And then in Phase 4, "How Is Data Protected?," officials will help to identify cybersecurity risks on a continuing basis, prioritize the risks based upon the severity of potential impacts, and mitigate problems.

The CDM program allows departments and agencies to carry out automated, ongoing, risk-based assessments of their cybersecurity. The CDM program allows for an expansion of continuous diagnostics by increasing the capacity of network sensors, increasing the collection of data from those sensors, and using that data to prioritize risk alerts. CDM offers agencies and departments a plethora of tools that can be updated as threats change.

A second goal of the CDM is to provide cost-efficient means to purchase resources to implement the cybersecurity program. To do this, the DHS and the General Services Administration in 2013 created a blanket purchase agreement (BPA) called the CDM Tools/Continuous Monitoring as a Service (CMaaS) BPAs. The purchase agreement allowed agencies to purchase continuous monitoring tools and services at a reduced cost. These tools enable the agencies to identify cyberthreats and then mitigate the impact of those threats.

Participating agencies install sensors that perform ongoing, automated searches for flaws in internet security. Results from the sensors are channeled into an agency dashboard that produces a customized report used to alert network managers to any critical online risks. These alerts allow agencies to efficiently allocate resources based on the severity of the risk. Progress reports track results, which can be used to compare security postures among agency networks. Within minutes, summary information is relayed to a federal dashboard and informs other agencies about any cybersecurity risks across the federal government. Mitigation mechanisms can then be implemented.

Those overseeing the program have designed it to ensure the privacy of any personal information. Any data that is transferred from the systems of CDM agencies to DHS does not include any personally identifying information (PII). It also does not include any information regarding computers in specific departments or agencies.

Another essential element of the CDM program is communication. The sharing of information is critical for successful security measures. Ongoing and ad hoc communications are both required as part of the CDM. Along with communication, the need for effective management cannot be overstated. There is a need for all agencies to have a common understanding of the basic concepts and principles that comprise CDM.

The federal government awards financial grants to help participating agencies and departments purchase needed tools. In July 2018, for example, the government awarded CGI Federal Inc. a six-year, $530-million contract to provide tools that will help agencies monitor cybersecurity risks. The company was founded in 1976 and works in conjunction with federal agencies to provide solutions for defense, civilian, health care, and intelligence.

Federal agencies and departments that elect to participate in the CDM program may save their department money by doing so. Many of the costs associated with the program will be paid by DHS, thereby reducing budget outlays for individual agencies.

See also: Cybersecurity; Personally Identifying Information

Further Reading

"CGI awarded $530 million Continuous Diagnostics and Mitigation contract to strengthen cybersecurity of federal agencies." *PR Newswire*, July 30, 2018. https://www.cgi.com/us/en-us/2018-07-30-CGI-awarded-530-million-Continuous-Diagnostics-and-Mitigation-contract-to-strengthen-cybersecurity-of-federal-agencies

Continuous Diagnostics and Mitigation Program, U.S. General Services Administration. https://www.gsa.gov/technology/technology-products-services/it-security/continuous-diagnostics-mitigation-cdm-program

Continuous Diagnostics and Mitigation, U.S. Computer Emergency Readiness Team. https://www.us-cert.gov/cdm/home

Delaney, David G. 2013–2014. "Cybersecurity and the administrative national security state: Framing the issues for federal legislation." *Journal of Legislation*, 40, pp. 251–279.

Office of Management and Budget (OMB). 2013. "Memorandum 14-03, enhancing the security of federal information and information systems," November 18, 2013. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf

COPYRIGHT INFRINGEMENT

Copyright is the exclusive right to print, publish, sell, or distribute a creative work, ranging from books to physical products to software and music. Copyright infringement (often referred to as piracy) occurs when a person uses a creative work that has been protected by copyright laws without the permission of the author or creator. When it comes to the internet, a copyright provides legal protection to the owner of a creative work should that creative work be illegally downloaded. When a person downloads music or books without paying for them, the author or creator does not receive the royalty, leading to financial loss. For example, in the early 2000s, peer-to-peer (P2P) file-sharing networks emerged, facilitating the illegal downloading and sharing of copyrighted works.

A related concept is intellectual property theft. Intellectual property refers to intangible property in which someone has an ownership right. In the United States, this not only includes copyrighted material but also patents and trademarks. Patents are designs to create a unique physical item or plans for a unique process of doing something. An example of a patent would be the designs for the manufacture of an iPhone. Trademarks are the distinctive logos and other design elements used by a business to identify itself. An example of a trademark would be Apple's logo, which is an apple with a bite taken out of it. As with copyrights, laws are in place to protect the owner of a patent or trademark should their intellectual property be used in an unauthorized fashion.

There are many reasons people would want to download music and movies from the internet. Most probably do so because it is free. Others may download items because they find that the product is not available in another format (i.e., it may be out of print or has been banned). In some cases, the individual may want to use the product immediately instead of purchasing it and waiting for the product to be shipped or going to a store to purchase the item. In some cases, the person may be able to get it on the internet before it is released to the public.

A recent trend is to download copyrighted material from a social media site such as YouTube and then upload it onto another site such as Facebook, without the permission of the creator. When this is done, it is called "freebooting."

IP theft and copyright violations have become extremely common on the internet, simply because it is easy to share files via social media or e-mails. It is simple to share files with other people. At the same time, it is difficult to track the offenders who are downloading the material. The problems are made worse by P2P sites. These allow files to be downloaded from the hard drives of other users. Once an item is on one user's network, anyone on that network will then have access to those files. Common P2P sites include Grokster, eMule, BitTorrent, Ares, Limeware, Morpheus, iTunes, Napster, Spotify, and SoulSeek. These sites help users share music, movies, software, or other items over the internet for free.

There are risks to file sharing. In some cases, the networks allow other members to have access to all files on another person's hard drive, including any private files. These networks also open up the opportunity for viruses and other malware to be installed in other computers. The malware may be attached to files that are downloaded by an unsuspecting user, and it may harm the computer or even the network. Software that is downloaded illegally is often of a lower quality than the real software. It often does not include many of the essential features of the original product, and the use will not have any documentation that is provided when the product is sold legally. In some cases, illegal software does not work effectively.

There has been a backlash against P2P sites. In 2000, the rock music group Metallica filed a lawsuit against Napster in the Northern District of California for providing a site where people could download music without paying for it. The judge in the case ordered Napster to remove all of Metallica's songs from its site. In 2005, MGM Studios filed a lawsuit against the P2P providers Grokster and StreamCast (*MGM Studios v. Grokster*, 544 US 903 (2005)). The Supreme Court noted that these services appeared to be marketing themselves as the replacements of Napster following its shutdown after the ruling from the district court in Northern California. The Supreme Court decided in favor of MGM, deciding that Grokster and StreamCast were providing illegal access to copyrighted materials.

As a way to prevent the theft of products and violation of copyright, some organizations look to see if a purchaser is complying with the software agreements and not downloading a product too often or sharing it with others.

It is difficult to place a value on the economic impact of copyright infringement and IP theft. These crimes are difficult to trace, and it is hard to put an estimate on the amount of illegally shared files. However, experts claim that copyright infringement costs billions of dollars each year to businesses from people who do not pay for the products. Additionally, the copyright holders also lose billions of dollars of profit each year.

IP theft and copyright violations are illegal under both federal and state law. In the United States, Congress has passed a series of laws to deter copyright infringement and IP theft. One of those is the No Electronic Theft Act, passed by Congress in 1997. This law set maximum penalties of up to five years in prison and a fine of up to $250,000. Congress also passed the Digital Millennium Copyright Act in 1998 that makes it a crime to disseminate any devices or services that are meant to evade methods that protect copyrighted materials. In 2008, Congress followed these laws with one entitled the Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act. In this law, Congress increased the civil penalties that could be applied in the case of infringement of copyright laws. It also increased the government's power to seize property from offenders.

Under these and other laws, a person who is found guilty of violating copyright laws may be prosecuted under either system. They can also be prosecuted civilly or criminally. If found to be criminally responsible, an offender may be sentenced to jail time and subject to fines. If found guilty of civil offenses, the victim could sue for monetary damages.

Other agencies are also fighting to protect copyrighted materials. The FBI created the National Intellectual Property Rights Coordination Center as a way to help fight intellectual property theft. The Center is overseen by the Department of Homeland Security, but it also works in conjunction with various law enforcement agencies, including Interpol and Europol, to fight against copyright infringement offenses.

See also: Digital Rights Management; Economy, Effects on; Entertainment, Effects on

Further Reading

Balganesh, Shyamkrishna. 2013. "Copyright infringement markets." *Columbia Law Review* 113, 8 (December): 2277–2332.

Jost, Kenneth. 2000. "Copyright and the internet: Should consumers download music and movies for free?" CQ Researcher, 10 (September 29, 2000): 769–792. http://library.cqpress.com/

Lemley, Mark A. and Reese, R. Anthony. 2004. "Reducing digital copyright infringement without restricting innovation." *Stanford Law Review*, 56, 6 (May): 1345–1434.

Staff Reporter. 2004. "Google is accused of copyright infringement." *Wall Street Journal*, November 22, 2004. https://www.wsj.com/articles/SB110109619963380645

CORPORATE ACCOUNT TAKEOVER

A corporate account takeover (CATO) is a type of electronic crime that is similar to identity theft for businesses. In these events, cybercriminals gain access and control over a business's bank accounts and finances and steal the login credentials and passwords of the company's officials, employees, or customers often through phishing activities or social engineering. To do this, the criminals may send an e-mail to employees that appears to be from a bank or other official business. If the employee opens the e-mail, malware is downloaded onto the employee's computer, which allows the criminal to track the employee's login information and passwords. The employee unknowingly provides sensitive information to the criminals. Some malware sends a message to the offender that the employee has logged on to the website; the offender is able to send a message to the user that the system is down or not responding. During the time the employee believes that the system is down, the offender is able to make transactions in the employer's name. In some cases, the offenders may target senior executives as a way to gain access to the files and accounts.

Once the thieves have access to the accounts, they are able to carry out unauthorized transactions in which they can steal money from the organization, resulting in substantial financial loss that may not be fully recovered. The criminals may also create fake employees, placing them on the payroll. They may also steal information pertaining to customers, or otherwise perform acts that harm the company's reputation. A CATO attack can be devastating to the victimized business.

This type of offense is a growing problem. Companies of all sizes have been affected, but they are especially dangerous for small businesses. Criminals target small businesses because they are less likely to have multiple security layers to protect their networks and accounts. Financial institutions are also at high risk of a CATO attack because of the large amounts of money that offenders can steal.

To protect themselves, cybersecurity experts advise, the owners of small companies should become more aware of ways to prevent these attacks and to mitigate the damages if an attack occurs. The owners should understand that it is important for businesses to make their employees aware of the dangers of opening e-mail attachments from unknown sources and know how to recognize e-mails that appear to be real. Businesses should provide training on internet safety to employees on a regular basis so they remain knowledgeable about threats and how to prevent them.

Businesses should also create relationships with banking institutions to help the bank identify attempts at unauthorized access or large money transfers. They can help to identify suspicious activity quickly. Banks can provide training and education programs for employees. Banks and other financial institutions often work alongside the U.S. Secret Service and the U.S. Federal Trade Commission (FTC) to prevent CATO attacks or mitigate the effects. Company officials should also employ software programs that secure their computers and networks, such as spam filters and antivirus software. Security updates should be installed as needed, and employees should use strong passwords that are difficult to steal.

See also: Malware; Phishing; Social Engineering

Further Reading

American Bankers Association. n.d. "The small business guide to corporate account takeover." http://www.aba.com/Tools/Function/Fraud/Pages/CorporateAccountTakeoverSmallBusiness.aspx

Ryckman, Pamela. 2012. "Owners may not be covered when hackers wipe out a business bank account." *New York Times*, June 13, 2012. https://www.nytimes.com/2012/06/14/business/smallbusiness/protecting-business-accounts-from-hackers.html

Sidel, Robin, and Tracy Ryan. 2014. "States, U.S. beef up cybersecurity training for bank examiners; Agencies also hiring information-technology experts." *Wall Street Journal*, November 30, 2014. https://www.wsj.com/articles/states-u-s-beef-up-cybersecurity-training-for-bank-examiners-1417392622

COSTS OF CYBERCRIME

Businesses around the world lose millions of dollars each year to cybercrime, either as victims of an attack or in taking measures to prevent and mitigate cybercrime. Individuals also spend a great deal of money to prevent falling victim or in losses due to the aftereffects of an attack. Estimates as to the costs of cybercrime vary. In 2015, Lloyds, the British insurance company, reported that businesses lost around $400 billion each year to cybercrime (Morgan, 2016). The Center for Strategic and International Studies based in Washington, D.C., estimated that the annual cost of cybercrime in the world economy was over $445 billion each year (Center for Strategic and International Studies, 2014). Another organization estimated that the cost of cybercrime to the global economy is over $450 billion (Hiscox, 2017). According to a study by Cybersecurity Ventures, the cost of cybercrime was estimated to be $3 trillion in 2015. They estimate that costs could rise to $6 trillion by 2021 (Paganini, 2016).

It is difficult to give exact figures on the costs of cybercrime to individuals, businesses, and organizations. Many cyberattacks may go unrecognized and therefore unreported. In other cases, a company may be unwilling to report an attack because of the potential for economic damage to the organization, but also because of a fear of reputational damage. People may wonder why the company was unable to prevent the attack, and then question the safety of their data and decide to shop elsewhere or use another company.

The costs of cybercrime incorporate many different components. One cost revolves around the expenditures related to deterring or preventing cybercrime. This can include the costs of software that are used to detect malware, or firewalls that are put into place to prevent a cyberattack, which can costs hundreds of dollars per year. It can also include training of personnel to help them understand how to avoid unwittingly uploading malware or other precautions to take to prevent a cyberattack. Cybercrime costs can also include activities take to detect if any malware has been uploaded into a computer system. Detection costs relate to those activities that organizations take in response to a threat of an attack to determine if an act is imminent. These are essential because they can deter an attack if a threat is taken seriously.

If an attack occurs, the costs of cybercrime are escalated by investigations that may be needed to discover the identity of the offender. In turn, this will also help to uncover the extent of the attack. An agency or organization will probably need to implement action to mitigate or lessen the effects of the attack. This may include repairing any harm to the agency's computer systems, or any loss to their customers. Some businesses may be required to spend significant funds to repair the company's reputation with the public. In the months after an attack, a business or organization will be forced to review its existing security measures and enhance security measures as a way to minimize any future attacks.

In addition to these costs, a cyberattack on a business or agency can lead to a loss of sensitive or confidential information pertaining to the business (i.e., trade secrets) or customers (credit card information or passwords). Chances are that in the period after an attack, there will be a disruption of the business as the company must spend time to recover from the attack. There could be an economic impact of that downtime or even a short time when the organization is unable to assist its customers in other ways as it repairs any equipment that was harmed or take measures to protect information.

Cybercrime affects businesses and organizations around the world, but it affects countries in different ways. According to the Ponemon Institute and HP Enterprise Security (2014), cybercrime affects businesses in the United States to a greater degree than in other countries. In 2014, the average costs of cybercrime to a company in the United States were $12.7 million, an increase of over a million from the previous year. The country with the second-highest average cost per company was Germany, where the value was $8.13 million. This was followed by Japan, with an average cost of $6.91 million; France was next ($6.38 million), followed by the United Kingdom ($5.93 million) and Australia ($3.99 million). The country with the lowest average cost of cybercrime per company was Russia, which experienced an average cost of $3.33 million (Poneman, 2014). The report also indicated that the average time a company took to return to normal after an attack was 45 days, which was longer than the 32 days in the previous year. Thus, the effects of cybercrime are becoming more costly and take longer to repair.

A similar study by on the cost of cybercrime by the Ponemon Institute in 2016 found the same trends. They indicated that companies in the United States had the highest average cost related to cybercrime when compared to companies in other countries. That year, the total annual cost of cybercrime in the United States was $17.36 million. This time, Australia had the lowest cost ($4.3 million). The country that showed the most significant increase in the costs of cybercrime was Brazil. Overall, the global cost of cybercrime was $73,750,667.

The Ponemon Institute report made it clear that cybercrime affects all industries. Not surprisingly, financial-related industries had the highest costs resulting from cybercrime at $16.53 million. Other industries that experienced losses included utilities and energy ($14.8 million); technology ($11.04 million); services ($8.99 million); industrial ($8.05 million); health care ($7.35 million); retail ($7.12 million); transportation ($6.81 million); public sector ($6.77 million); communications ($6.13 million); consumer products ($5.80 million); media ($5.75 million); pharmaceutical ($4.92 million); education and research ($4.45 million); hospitality ($3.68 million); automotive ($3.56 million); and agriculture ($2.77 million) (Ponemon Institute, 2016, p. 7).

That same 2016 Ponemon survey of 237 organizations across six countries shows that almost all the companies included in the study had experienced a cyberattack of some kind. The attacks ranged from malware attacks to ransomware, phishing and social engineering attacks, DoS attacks, Web-based attacks, and botnets. The authors of the study concluded that companies with a high security profile will experience lower costs related to cybercrime when compared to those who take fewer security measures. The study also found that the most significant financial impact of a cyberattack to a business is the loss of information. This indicates the need for businesses and agencies to take efforts to reduce the potential for the loss of information by regularly backing up their data so it is available if a cyberattack should occur (Ponemon, 2016).

A separate study of 3,000 companies discovered that many companies and agencies are not prepared to deal with the fallout of a cyberattack on their company if one occurs. They estimated that the cost of cybercrime to the global economy is over $450 billion (Hiscox Cyber Readiness Report, 2017).

The loss to businesses from cybercrime can include the cybercriminal who seeks to hack into a computer system to steal data or customer information, but can also be from current or former employees who seek to harm the company. An example is Sam Yin, who was a computer expert for Gucci's U.S. headquarters in New York. He was fired from his job in May 2010 for using his employee discount to purchase $100,000 in luxury goods. He hacked into the company's computers and was able to delete everything in employee mailboxes and shut the system down for a day. In addition, top employees were prevented from being able to retrieve documents for months after the attack. He did this by creating a false account that remained active even after he was fired from the company. He was charged with 50 offenses, including computer tampering, identity theft, falsifying business records, computer trespass, criminal possession of computer-related material, unlawful duplication of computer-related material, and the unauthorized use of a computer. In all, he faced 15 years in prison. Yin pled guilty to some of the charges and was given a sentence of two to six years in prison. Upon his sentencing, the judge remarked, "A white-collar criminal does as much damage to society as a robber, a burglar or an assailant." It was estimated that Yin caused an estimated $200,000 in damages to the company in damage and lost productivity.

It is not only businesses that suffer losses after a cyberattack. The potential for loss for consumers is very high. They can lose personal information or intellectual property; they can also lose financially through an attack on bank accounts; they may also suffer damage to their computer. The average cost per victim has risen by 50 percent in the past 12 months.

There are few people who would argue that the costs of cybercrime will continue to rise in the future. As more companies, organizations, and individuals rely on computers for daily activities, the need to prevent and deter cybercrime is expected to increase, along with the costs of doing so.

It is essential that businesses rely on a practice called continuous monitoring, whereby executives rely on technology to discover risk concerns in their computer systems. This allows officials to detect potential weaknesses so that they can be fixed or patched before a cybercriminal can take advantage of the vulnerability. In the end, continuous monitoring is a way to protect a company's assets (data or secrets) from a potential cyberattack. As the term implies, the monitoring must be continuous or constant because the threats are constantly changing and becoming more complex. These techniques must often be implemented by multiple departments in order to be most effective.

See also: Bots and Botnets; Hacker and Hacking; Malware; Ransomware

Further Reading

Anderson, Ross, Chris Barton, Rainer Bohme, Richard Clayton, Micel J. G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. 2013. "Measuring the cost of cybercrime." In *The Economics of Information Security and Privacy*, Ranier Bohme, ed. Munster, Germany: Springer, pp. 265–300.

Bernik, Igor. 2014. "Cybercrime: The cost of investments into protection." *Journal of Criminal Justice and Security* 16, 2 (June 1, 2014): 105–116.

Center for Strategic and International Studies. 2014. "Net losses: Estimating the global cost of cybercrime." https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/McAfee%20and%20CSIS%20-%20Econ%20Cybercrime.pdf

Fisher, Janon. 2012. “Disgruntled Gucci computer whiz who crashed company’s email system sentenced to 2 to 6 years.” *New York Daily News*, September 10, 2012. www.nydailynews.com/new-york/disgruntled-gucci-computer-whiz-crashed-company-email-system-sentenced-2-6-years-article-1.1156062

Hiscox. 2017. “The Hiscox cyber readiness report.” https://www.hiscox.co.uk/cyber-readiness-report/

“How much is cyber crime costing U.S. businesses?” 2015. *Security: Solutions for Enterprise Security Leaders*, February 1, 2015, p. 12. https://www.securitymagazine.com/articles/86066-how-much-is-cyber-crime-costing-us-businesses

Italiano, Laura. 2012. “Ex-staffer sentenced to 2–6 years for hacking into Gucci’s system.” *New York Post*, September 10. https://nypost.com/2012/09/10/ex-staffer-sentenced-to-2-6-years-for-hacking-into-guccis-system/

Kondakci, Suleyman. 2009. “A concise cost analysis of internet malware.” *Computers and Security*, 28: 648–659.

Leyden, John. 2011. “Fired Gucci IT worker accused of tearing up network.” *The Register*, April 5, 2011. https://www.theregister.co.uk/2011/04/05/gucci_bofh_revenge_hack/

Morgan, Steve. 2016. “Cyber crime costs projected to reach $2 trillion by 2019.” *Forbes*, January 17, 2016. https://www.forbes.com/sites/stevenmorgan/2016/01/17/cyber-crime-costs -projected-to-reach-2-trillion-by-2019

Moscaritolo, Angela. 2011. “Former Gucci insider charged with hacking network.” *SC Media*, April 5, 2011. https://www.scmagazine.com/former-gucci-insider-charged-with-hacking-network/article/558806/

Paganini, Pierluigi. 2016. “Global cost of cybercrime will grow from $3 trillion in 2015 to $6 trillion annually by 2021.” *Security Affairs*, August 28, 2016. http://securityaffair.co/wordpress/50680/cyber-crime/global-cost-of-cybercrime.html.

Ponemon Institute. 2016. “2016 cost of cyber crime study and the risk of business innovation.” https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf

Ponemon Institute and HP Enterprise Security. 2014. “2014 global report on the cost of cyber crime.” October 30, 2014. https://www.ponemon.org/library/2014-global-report-on-the-cost-of-cyber-crime

Sans Institute. n.d. “Continuous monitoring: What it is, why it is needed, and how to use it.” https://www.sans.org/.../analyst/continuous-monitoring-is-needed-35030

COUNCIL OF EUROPE CYBERCRIME CONVENTION

In response to concerns over the development and expansion of criminal offenses related to computers and the internet, the Council of Europe (CoE) created the Cybercrime Convention in November 2001, sometimes referred to as the Budapest Convention. The treaty is the first binding international agreement that focuses on investigating crimes committed through the internet and punishing offenders. The aim of the treaty is to have synchronized or harmonized international laws against cybercrime that will also improve investigative abilities of law enforcement agencies through increase international cooperation, with international investigations and prosecution of cyber criminals. In short, the main goal of the treaty’s creators was to establish a “common criminal policy” to attack computer-related crimes.

As new criminal offenses related to computers and the internet developed, it quickly became apparent that a global approach to solving cybercrime would be needed if there was to be an effective war on cybercrime. Cybercriminals did not respect national boundaries, and cybercrime did not affect victims in only one jurisdiction. Instead, cybercrime was a worldwide phenomenon that required an international response from law enforcement agencies. A country-by-country or state-by-state response to cybercriminals simply would not be an effective attack on cybercriminals.

Initial discussions about a possible treaty concerning cybercrime began in 1997 after a series of harmful computer viruses spread to computers around the world and few offenders were ever prosecuted for their actions, if they were even identified. That year, the CoE appointed a Committee of Experts on Crime in Cyberspace that was responsible for identifying new crimes, jurisdictional rights, and criminal liabilities associated with the internet. Canada, Japan, South Africa, and the United States were also invited to participate in the discussions as observer nations.

If states sign and ratify the treaty, they are not obligated to accept all provisions of the treaty. Instead, they can pick and choose what provisions they choose to enforce. However, if a country signs on to the treaty, they agree to certain things. They agree to define or create laws and sanctions within their criminal codes for four categories of computer-related crimes: fraud and forgery, child pornography, copyright infringements, and security breaches (including hacking and the dissemination of malware that compromises the integrity of a network or data). The country also agrees to create laws that outline their jurisdiction over these offenses if the crimes are committed within their country's boundaries, or if they occur on registered ships and aircraft, or by their citizens when they are staying abroad. Countries agree to establish specific procedures for detecting, investigating and prosecuting those who intentionally commit cybercrimes by collecting and preserving of evidence. By signing, countries also agree to create a system for international cooperation for extraditing offenders.

The organization adopted the Cybercrime Convention in November 2001. Twenty-six member states signed the convention in Budapest, Hungary (thus the reference to the Budapest Convention). As of April 2018, 57 states have ratified the document while others have signed but not ratified the document. Both member states and nonmember states have been asked to participate. To date, only two member states oppose the convention and have refused to sign it: Russia and San Marino. Two nonmember countries signed on to the treaty but did not formally ratify it (Canada and South Africa). Two other nonmember states have ratified the treaty (the United States and Australia). Six member states have signed but not ratified.

If a country agrees to participate in the treaty, it agrees to provide international cooperation to other countries when computer-related crimes occur. It must provide a contact that will assist another country if it needs help investigating a computer crime. The treaty provides police agencies with expanded powers to investigate cybercrimes when the offense crosses national borders.

The treaty is divided into four chapters. Each of the chapters comprises articles, or provisions, that describe a particular element. In all, there are 48 articles in the treaty. The first chapter defines relevant terms related to cybercrime. The first section of Chapter 2 outlines four broad categories of cyberoffenses. They are: (1) offenses against the confidentiality, integrity, and availability of computer data and systems; (2) computer-related offenses; (3) content-related offenses (i.e. child pornography); and (4) Offenses relating to copyright infringement. The second section of Chapter 2 looks more at the procedural aspects of the law, particularly because countries vary a great deal with regards to how the laws will be implemented and by whom. On the whole, this chapter is an attempt by the authors to make sense of the laws on cybercrime and make them more consistent among participating countries so that cybercrimes can be investigated and prosecuted more effectively.

Chapter 3 of the treaty highlights international cooperation among the international community, describing jurisdictional boundaries. The chapter also focuses extensively on extradition and mutual assistance. Chapter 4 addresses procedural matters and methods for settling disputes.

Of the 48 articles that the treaty comprises, 33 require nations who ratify it to adopt or create some kind of legislation that will create a new criminal offense. In most countries that already have some kind of laws banning cybercrime, this is relatively easy to do. In those countries that have done little to regulate cybercrime, it will be a more difficult task. This is also a difficult task in some countries because of cultural differences. Another problem is the period of time from when the Convention was first passed to the present. Many of the technologies that were commonly used when the document was originally drafted are now out of date and not relevant. Instead, they have been replaced with new technology that may not be addressed in the treaty (Brenner, 2007).

Some supporters posit that the treaty will deter cybercriminals because offenders will be more likely to be caught and punished if they commit crimes that harm businesses or individuals—it will no longer be easy to hide in another jurisdiction after committing a crime. They agree that if sanctions are used more regularly against offenders, some offenders may not commit an offense. They may also be deterred if there is little opportunity for an offender to operate out of a country where there are lax policies and where they know they won't be caught or punished.

Most participants agree that the convention will only work if all countries adopted the treaty and implement it. There must be cooperation and participation from law enforcement around the world. This is especially true of those countries where there is currently only limited enforcement of laws and cybercriminals are able to operate with little government intervention.

There are opponents to the treaty, or some who are hesitant to support it. Many opponents have expressed their concerns about the impact of the treaty on privacy rights of individuals and their civil liberties. They argue that the increased surveillance powers given to law enforcement is too great. They point out that under the treaty, law enforcement will be able to search individuals and their property in situations that are currently banned in the United States. It will also allow law enforcement to send personal data to another country where they may not support the civil rights of their citizens.

The treaty was amended in March 2006, when the Additional Protocol to the Convention on Cybercrime was passed. States that have ratified this agree to pass laws to make it illegal to disseminate racist and xenophobic material through the internet.

See also: Child Pornography; Federal Bureau of Investigation; Interpol

Further Reading

Archick, Kristin. 2003. "Cybercrime: The Council of Europe convention." In *Cybercrime and cyberterrorism: Current issues*, edited by John V. Blane. New York: Novinka Books, pp. 1–6.

Brenner, Susan W. 2007. "Cybercrime: Rethinking crime control strategies." In *Crime online*, edited by Yvonne Jewkes. Devon, UK: Willan Publishing, pp. 12–28.

Brenner, Susan W. 2011. "Defining cybercrime: A review of federal and state law." In *Cybercrime: The investigation, prosecution, and defense of a computer-related crime*, edited by R. D. Clifford. Durham, NC: Carolina Academic Press.

Clough, Jonathan. 2015. *Principles of cybercrime*. Cambridge, UK: Cambridge University Press.

Gillespie, Alisdair A. 2016. *Cybercrime: Issues and debates*. New York: Routledge.

Weber, A. M. 2003. "The Council of Europe's convention on cybercrime." *Berkley Technology Law Journal*, 18: 425–446.

CRACKER AND CRACKING

"Cracker" is a term that refers to a person who breaks into a computer system or breaches computer security in an attempt to commit criminal or harmful acts such as stealing data. They may disable features such as copy protection so they can copy software. In some cases, the cracker will break into a system for profit or to steal data such as credit card numbers. While they have malicious intent, crackers usually cause less harm than hackers because they are not professionals and do not have much knowledge about computers. They are sometimes referred to as "black-hat" hackers, who intend to commit harm.

Crackers are usually successful because they are persistent. They will try many different ways to find and exploit a weakness in a computer system's computer code. They will sometimes attempt to trick people into giving them passwords or other personal information. They may pretend to be an employee in the agency, or send an e-mail that appears to be an official communication from a bank or an IT department. Another technique used by crackers is to look for a "backdoor" to find a way into a program, and then exploit the back door.

A cracker can be distinguished from a hacker, who is a person who breaks into a computer system to learn more about the system or network. Those who identify as being crackers usually want to know how it works, and generally have an advanced knowledge of computers. Often a hacker is a professional who has permission to break into a system to look for vulnerabilities so they can be patched. They are often hired by companies to identify flaws in a security system in an attempt to fix them. Hackers do not respect crackers.

One of the most famous crackers was David Mitnick, who started hacking into computer systems at the age of 12 in order to get a bus pass in Los Angeles. Mitnick became a "phone phreaker" who broke into the computers of Digital Equipment Corporation and Pacific Bell. He was apprehended and charged with multiple offenses, including multiple counts of unauthorized access to a federal computer, wire fraud, possessing unauthorized access devices, interception of wire or electronic communications, unauthorized access to a federal computer, and causing damage to a computer. He served about five years in prison for these offenses.

While some people will argue there is a difference between the terms "cracker" and "cracking," most people use the terms interchangeably and do not distinguish between them.

See also: Backdoor; Black-Hat Hackers; Hacker and Hacking; Mitnick, Kevin

Further Reading

Dittrich, David, and Kenneth Einar Himma. 2006. "Hackers, crackers and computer criminals." In *Handbook of information security*, edited by Hossein Bidgoli. New York: John Wiley and Sons, pp. 154–171.

Dogaru, Olguta. 2012. "Criminological characteristics of computer crime." *Journal of Criminal Investigation* 5, 1: 92–98.

Richet, Jean-Loup. 2013. "From young hackers to crackers." *International Journal of Technology and Human Interaction* 9, 3: 53–62.

Smith, Alan D and William T. Rupp. 2002. "Issues in cybersecurity; Understanding the potential risks associated with hackers/crackers." *Information Management & Computer Security* 10, 4: 178–183.

CRAIGSLIST KILLERS

Since the development of Craigslist, an internet site for classified ads, criminals have taken advantage of the site to make contact with other users, sometimes resulting in death. The term often used when a victim and offender meet online and arrange a meeting through an online ad or chatroom is "internet homicide." There have been multiple murders that have resulted from contacts made through Craigslist.

Craigslist is an internet website on which people can post classified ads. Individuals can place ads for jobs, housing, items they have for sale, or just about anything else. The site was founded in 1995 and has been beneficial for thousands of people, but it has also been linked to hundreds of rapes, murders, and robberies. A study by Advanced Interactive Media Group found that over 100 murders, rapes, and robberies have been committed through Craigslist meetings (Dewey, 2016). In these cases, offenders arrange meetings with victims using the pretense of buying or selling an item or discussing a possible job opportunity.

One of the first murders associated with Craigslist occurred in Minnesota in October 2007. College student Michael Jon Anderson, 19, met Katherine Ann Olson, 24, through Craigslist. Katherine wanted to earn money to pay for graduate school, and she responded to an ad placed by a woman named Amy to babysit her daughter. Katherine made a comment to her roommate that Amy seemed odd on the phone, but she decided to go anyway. When Katherine showed up at Amy's apartment to babysit, Amy was not there. Instead, she was met by Anderson, who shot Katherine in the back of her head. In the end, Anderson was found guilty of first-degree murder. He was given a life sentence without parole on April 1, 2009.

A more well-known crime spree that involved Craigslist was carried out by Philip Markoff in April, 2000. This turned out to be one of the most notorious Craigslist crimes. Markoff's offenses began on April 10, when he bound and gagged a masseuse/escort named Trisha Leffler. Leffler had advertised her services on Craigslist. Markoff arranged to meet Leffler at the Westin Copley Place in Boston, Massachusetts. During their meeting, he robbed her at gunpoint. A few days later on April 14, Julissa Brisman was found dead in the same hotel. She had placed an ad on Craigslist in the Exotic Services section describing her services as a "masseuse." She had been beaten and shot three times. On April 16, erotic dancer Corinne Stout became a victim of an attempted robbery at a Holiday Inn Express in Warwick, Rhode Island. Markoff had a weapon and was attacking Stout when he was interrupted by the victim's husband. He pointed the gun at the pair but ran off before using it.

It wasn't long before law enforcement charged Markoff with the crimes. Officials discovered that he was a second-year medical student who allegedly arranged to meet the victims through ads on Craigslist. Law enforcement officials in Massachusetts arrested Markoff on April 20, and he was arraigned the next day in the Boston court system, pleading not guilty to charges relating to the murder of Brisman. On March 4, officials in Rhode Island issued a warrant for his arrest. When police arrested Markoff, they searched his apartment and found a semiautomatic weapon, duct tape, wrist restraints, and other items that were used in the crimes.

A grand jury indicted Markoff in June, 2009 for first-degree murder, armed robbery, and other criminal charges. While held in jail before the trial, Markoff attempted suicide multiple times. Markoff took his own life on August 5, 2010, while in jail. In 2011, the Lifetime television network released a movie based on Markoff's alleged crimes, titled *The Craigslist Killer*.

Another event related to Craigslist occurred in Ohio in November, 2011. Sixteen-year-old Brian Rafferty and 52-year-old Richard Beasley placed an ad on Craigslist expressing their interest in hiring a farm assistant who would care for cattle on a 688-acre property for $300 a week. Over 100 people expressed an interest in the position. The first person to respond to the ad was David Pauley, from Norfolk, Virginia. When Pauley traveled to Ohio to interview for the position, Rafferty and Beasley shot and killed him.

Later that year, Rafferty and Beasley lured another victim to Ohio through Craigslist. The men placed another ad in which the pair sought a farm assistant, to which Scott Davis, of South Carolina, responded. Davis met Rafferty and Beasley on November 6, and they all walked a short distance through a wooded area. However, Rafferty then pointed a gun at Davis. When Davis fled, Rafferty shot him in the arm. Rafferty hid in the woods for seven hours, eventually approaching a nearby house for help. The homeowner called 911 and the local police.

On November 13, Rafferty and Beasley picked up their third victim, Timothy Kern, 47, at a pizza shop near Massillon, Ohio. Kern, a father of two young boys, had recently lost his job and was seeking employment. Beasley shot Kern five times, killing him. By then, Rafferty's family had reported him missing, and along with the information from Davis, the local sheriff's office began to investigate possible wrongdoing. They worked jointly with the FBI and were able to link Beasley and Rafferty with the crimes. Authorities arrested Beasley and Rafferty on November 16.

Rafferty was charged with one count of attempted murder and one count of complicity to attempted murder. He was tried as an adult and sentenced to serve a life sentence without parole. Beasley was convicted for killing Pauley and Kern, and a third man named Ralph Geiger whom Beasley killed for the purpose of stealing his identity. He was also found guilty for the attempted murder of Scott Davis.

One final example of a Craigslist murder took place in March 2009 when 16-year-old John Katehis murdered popular ABC radio news reporter George Weber, 47, in New York. Katehis placed an ad on Craigslist in which he advertised his sexual services. At the same time, Weber posted that he was looking for sexual services. Katehis stabbed Weber 50 times, claiming self-defense because Weber attacked him first. Katehis was arrested and confessed to the crime. He was found guilty of murder and sentenced to serve 25 years to life in prison.

Craigslist has been criticized for providing a forum for criminal activity. However, officials at Craigslist deny any responsibility for any of these crimes.

See also: Cyberstalking; Federal Bureau of Investigation

Further Reading

Dewey, Caitlin. 2016. "Think twice before answering that ad: 101 murders have been linked to Craigslist." *The Washington Post,* January 11, 2016. https://www.washingtonpost.com/news/the-intersect/wp/2016/01/11/think-twice-before-answering-that-ad-101-killers-have-found-victims-on-craigslist/?noredirect=on&utm_term=.9003b95de69b

Ford, Beverly, Nancy Dillon, and Tracy Conner. 2009. "Surviving victim of Craigslist killer: Phillip Markoff should be jailed for life." *NY Daily News*, April 23, 2009. http://www.nydailynews.com/news/surviving-victim-craigslist-killer-phillip-markoff-jailed-life-article-1.362281#

Goode, Erica. 2011. "Craigslist used in deadly ploy to lure victims in Ohio." *New York Times*, December 2, 2011. https://www.nytimes.com/2011/12/02/us/three-lured-to-death-in-ohio-by-craigslist-job-ad.html

McPhee, Michele, Dean Schabner, and Nikki Battiste. 2010. "'Craigslist Killer' Philip Markoff commits suicide." ABC News, August 15, 2010. https://abcnews.go.com/US/craigslist-killer-phillip-markoff-commits-suicide/story?id=11405484

Rosin, Hanna. 2013. "Murder by Craigslist." *The Atlantic*, September 2013. https://www.theatlantic.com/magazine/archive/2013/09/advertisement-for-murder/309435/

CREDIT CARD FRAUD

The term “credit card fraud” refers to any theft or fraud committed with or by using a stolen credit card or debit card to make unauthorized purchases or withdraw funds from another person’s account. Cybercriminals steal personal and financial data from another person and then use that for illegal activities. They can make CNP (card not present) purchases that are carried out without the physical card, which can be made when a person uses the card numbers and information but does not show the actual card. These are purchases made via an online website, over the phone, or through the mail. The offender will often purchase high-end products such as technology and then resell the product to make a significant profit. Some offenders use the stolen information to make a fake card, which is used to make purchases in stores or other outlets. Often, the stolen credit card information is sold on the internet to other criminals. Credit card fraud can result in great financial loss for both the credit card company and for the individuals whose information is stolen.

It has been estimated that around 0.1 percent of all credit card transactions are fraudulent (Bennett, 2015). Many breaches have been attributed to criminal organizations who steal the information and then sell it on the dark web. The information from a good credit card can sell for an average of $21 (Taylor, 2016). One criminal organization, called FIN6, has developed a reputation for its ability to steal credit card information and then sell it on the dark web. They do not use the card information to make illegal purchases but instead sell the information to others. This group is known for its ability to get the stolen information on the market quickly, before it can be reported as stolen. They do this because current card information is worth more than card information that has been available for a longer period of time (Schwartz, 2016).

There have been many well-publicized incidents of credit card fraud. In 2013, the retail store Target’s system was breached, and the data of 40 million customers was stolen, including names, credit card numbers, expiration dates, and security codes. That same year, payment card data that had been stored on company computers was stolen from Neiman Marcus. In 2014, an attack on Home Depot led to the possible theft of card information from 56 million customers. In May 2016, criminals stole data from the South African Standard Bank Group and used that information to create fake credit cards. The criminals made about 1,600 cards and used them to withdraw $13 million in cash from cash machines located throughout Japan. They withdrew about $913 in each withdrawal, the maximum amount allowed per each transaction. In all, they made 14,000 transactions.

Credit card fraud is difficult to stop. Often, the card holder is unaware that their card has been stolen and used fraudulently, giving thieves time to make purchases. It is also difficult to identify the offender and recover any stolen goods or funds. Many offenders work in countries where the laws don’t cover these acts or where law enforcement does not enforce the laws vigorously. The offenders also move around a lot so it is difficult to locate them. In all, credit card fraud is a relatively easy crime to carry out, and there is a low chance of being convicted for it.

There are many methods that offenders use to commit credit card fraud. Offenders can commit credit card fraud through the use of malware (malicious software) such as worms, viruses, or Trojans. A criminal will install malware onto a company's website so that when the victim uses the website, the malware is unknowingly downloaded onto the user's computer. The malware allows the offender to have access to the victim's personal information on that computer, including the victim's e-mails, bank accounts, and even passwords.

For example, a criminal may install a keylogger that will track every keystroke a victim makes on the keyboard. From this, the offender can access credit card and account information directly from a victim's computer. Or an offender may use a phishing attack whereby a victim will receive an e-mail that appears to be from a legitimate company or organization that is seeking the victim's personal information. The e-mail may appear to be from a bank, indicating that there is a problem with an account. The victim is tricked into providing details that the criminal can use to steal money. In some cases, there is an attachment to the e-mail, and when the victim clicks on the attachment, malware is installed on the computer that allows the offender access to information. This type of social engineering allows an offender to steal the card information through contact with the individual.

Credit card numbers have also been stolen in person, such as restaurant employees copying the numbers on a card or even using carbon paper to steal the information, a practice called "manual credit card imprints." There have also been cases in which a merchant or seller has worked with offenders to steal credit card information from a customer.

Other offenders have used card skimming devices to acquire the numbers. These can be placed on any payment device, but they are often found on gas pumps, in ATMs, or in restaurants and bars. Skimmers are small devices that are attached to a card swipe device. When a customer swipes their card, the device stores the card numbers and information. If the device is on the swipe device for an extended time, it can steal the numbers off of hundreds of cards. A similar technique is a keypad overlay, which is placed on a keypad. When the keypad is used by a victim, the information is wirelessly transmitted to the offender.

Criminals sometimes steal cards when they are sent to a customer through the mail. In this case, the legitimate card holder never receives the card, so he or she is unaware that the card has been stolen and does not report the theft. A similar technique is application fraud, whereby a criminal applies for a credit card using another person's name and information that they are able to steal from other information or from online sources.

Once the information from a credit card is stolen, the offender is able to carry out an "account takeover." This occurs when an offender uses the stolen card information to report that the card has been stolen and then requests a change of address. A new card will come in the mail and can be used by the offender for fraudulent purchases. Thus the offender takes over the account and makes transactions on it without the permission of the owner.

In an attempt to stop the theft of credit card numbers, most credit card companies are now placing an EMV chip on cards instead of raised numbers, which are much easier to steal. Cardholders can also make efforts to protect themselves from the theft of card data, such as checking accounts regularly for suspicious activity, reporting lost or stolen cards, updating virus protection software, and avoiding opening any e-mails from suspicious sources. Merchants can also take action to reduce the opportunity for credit card fraud. They can issue receipts that do not print the credit card numbers on them. They can also request identification from people who are using credit cards to make purchases and install updated antivirus programs to ensure their systems do not have malware on them.

A new proposal to combat credit card fraud is a virtual credit card. The card functions as a traditional card in that the numbers on a card are linked to an account. However, the card can only be used once, either at a merchant or online, after which time the card will expire. In some cases, a customer can have a different credit card number for every retailer. This will limit the possible damage if the data is stolen.

See also: Identity Theft; Malware; Phishing

Further Reading

Bennett, Michael. 2015. "11 types of credit card fraud." *Consumer Protect*, September 28, 2015. https://www.consumerprotect.com/11-types-of-credit-card-fraud

Hand, D. J., C. Whitrow, N. M. Adams, P. Juszczak, and D. Weston. 2008. "Performance criteria for plastic card fraud detection tools." *Journal of Operational Research Society* 59, 7 (July): 956–962.

Koren, James Rufus. 2017. "These firms have a novel solution to online fraud: Disposable credit card numbers." *Los Angeles Times*, November 27, 2017. www.latimes.com/business/la-fi-agenda-virtual-cards-20171127-htmlstory.html#

Schwartz, Mathew J. 2016. "Cybercrime gang tied to 20 million stolen cards." *Bank Info Security*, April 21, 2016. http://www.bankinfosecurity.com/cybercrime-gang-tied-to-20-million-stolen-cards-a-9058.

Taylor, Harriet. 2016. "What one criminal gang does with stolen credit cards." CNBC, April 20, 2016. http:///www.cnbc.com/2016/04/20/what-one-criminal-gang-does-with-stolen-credit-cards.html.

CRYPTOCURRENCY

A cryptocurrency is a digital currency that is decentralized. In other words, there is no centralized entity, such as a bank, that is responsible for regulating monetary transactions. Rather, cryptocurrencies have decentralized regulation. This means that several nonrelated individuals or other entities track and keep record of the transactions.

Bitcoin is by far the largest cryptocurrency in circulation, and it is also deemed to be the first cryptocurrency. Some of the larger cryptocurrencies include Ethereum, Dash, Moreno, Ripple, and Litecoin (Hileman and Rauchs, 2017). It is estimated that over 200,000 Bitcoin transactions and between 40,000 and 50,000 other cryptocurrency transactions take place each a day (Hileman and Rauchs, 2017). This brings in millions of dollars of revenue for digital currency exchanges, with some of the top exchanges making in excess of $3 million a day (Russo, 2018).

There are a number of countries that prohibit the use of cryptocurrencies. Eight countries—Algeria, Bolivia, Egypt, Iraq, Morocco, Nepal, Pakistan, and the United Arab Emirates—explicitly ban the use of cryptocurrencies. Another 15 countries—Bahrain, Bangladesh, China, Columbia, the Dominican Republic, Indonesia, Iran, Kuwait, Lesotho, Lithuania, Macau, Oman, Qatar, Saudi Arabia, and Taiwan—implicitly ban the use of cryptocurrencies (Law Library of Congress, 2018). Even among those countries that do permit the use of cryptocurrencies, many regulate that use. In the United States, some cryptocurrencies—depending on how they are structured—may be deemed to be securities by the Securities and Exchange Commission (SEC). When determining whether a cryptocurrency is a security, one thing the SEC looks at is whether the sale of the cryptocurrency constitutes "a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party" (*Securities and Exchange Commission v. W. J. Howey Co. et al.*, 328 U.S. 293 (1946)). Companies that exchange such cryptocurrencies are required to register with the SEC (U.S. Securities and Exchange Commission, 2018). A number of countries hold cryptocurrencies subject to tax regulation, anti-terrorism, and money laundering regulations (Law Library of Congress, 2018).

Cryptocurrencies prove to be particularly susceptible to use in criminal enterprises due to the fact that cryptocurrencies are generally not traceable to a given individual, if an individual takes the proper precautions (Federal Bureau of Investigation, 2012, p. 5). Because of this, it is possible for someone to use these currencies to purchase illegal goods or services without fear of the transaction being traced back to them. One website, Silk Road, was specifically used to conduct illegal transactions, and before it ultimately shut down, it used Bitcoin for transactions that took place on the site (Greenberg, 2013). Use of cryptocurrencies in criminal activity, however, extends beyond just one website. It is estimated that half of all Bitcoin transactions involve illegal activity, resulting in around $72 billion of annual illegal activity (Foley et al., 2018).

Cryptocurrencies are also susceptible to theft. Where cryptocurrencies are decentralized, the FBI assessed that those who used cryptocurrencies could be vulnerable to theft of their cryptocurrencies. A thief would only have to hack into and compromise the personal computer of a cryptocurrency user to commit a theft, as opposed to having to hack into and compromise the computers of a large company—such as a bank or other financial institution—to commit a theft (Federal Bureau of Investigation, 2012).

See also: Bitcoin; Digital Currency; Silk Road

Further Reading

Federal Bureau of Investigation. 2012. *Bitcoin virtual currency: Intelligence unique features present distinct challenges for deterring illicit activity*. Federal Bureau of Investigation, April 24, 2012.

Foley, Sean, Jonathan R. Karlsen, and Tālis J. Putniņš. 2018. "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?" Social Science Research Network. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645

Greenberg, Andy. 2013. "Founder of drug site Silk Road says Bitcoin booms and busts won't kill his black market." *Forbes*, April 16, 2013. https://www.forbes.com/sites/andygreenberg/2013/04/16/founder-of-drug-site-silk-road-says-bitcoin-booms-and-busts-wont-kill-his-black-market/#634bddae6c42

Hileman, Garrick, and Michel Rauchs. 2017. *Global cryptocurrency benchmarking study*. Cambridge, UK: Cambridge Centre for Alternative Finance.

Law Library of Congress. 2018. *Regulation of cryptocurrency around the world*. Washington, D.C.: Law Library of Congress.

Russo, Camila. 2018. "Crypto exchanges are raking in billions of dollars." *Bloomberg*, March 5, 2018. https://www.bloomberg.com/news/articles/2018-03-05/crypto-exchanges-raking-in-billions-emerge-as-kings-of-coins

U.S. Securities and Exchange Commission. 2018. "Statement on potentially unlawful online platforms for trading digital assets." U.S. Securities and Exchange Commission, March 7, 2018. https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading

CRYPTOGRAPHY

There are times when a sender may want to send data or information to another person electronically but also wants to ensure the safety or privacy of that information. In other words, the sender may want to ensure that if a third, unauthorized person intercepts that information while it is being sent, the third party would not be able to understand the data or alter it in some way. Cryptography is a way to hide the meaning of the data. It is used to keep information private or confidential, inaccessible from anyone who should not have access to it or otherwise use it to harm others. The receiver must have a key in order to understand the data. Cryptography can also help a sender determine if data has been altered. This way, the integrity and authenticity of the data is maintained.

Cryptography has been used for many years to hide information or messages from others. Today it is relied on to protect private information such as health records or financial information that is sent online. The safety of this information is critical for e-commerce to work smoothly. Otherwise, no one would have confidence to order or purchase items online. This technology is used regularly by those in industry and commerce, private agencies and organizations, medical facilities, and financial institutions.

With cryptography, data (called plain text) is converted through the use of a mathematical algorithm, or encryption algorithm, into a cipher text that can be sent to another person or stored. At that point, the data is considered to be encrypted. This means that the data is scrambled in such a way that it is unreadable by a third party. The recipient of the data must be provided with a secret key (a decryption algorithm) that is used to decipher or unscramble the coded data and return it to an easy-to-read, plain text. If done correctly, only the recipient can decode the data. Any third parties who may want to have unauthorized entry, often called interceptors or attackers, are blocked from doing so.

Of course, there are those who seek to break the code and have access to the cipher text. The practice of breaking the cipher text is called cryptanalysis. They focus on ways to decode transmitted data. Sometimes, cryptanalysis can also be used to test the strength of an algorithm to ensure it is transmitting data securely.

There are two types of cryptosystems. The first is the symmetric key encryption, or conventional encryption or single-key encryption, and the second is asymmetric key encryption. With the first type of encryption, symmetric key encryption, the same keys are used by both the sender and receiver to encrypt and decrypt the data. The sender and receiver share a common key. That key is changed often as a way to prevent an attacker from accessing the data. This type of cryptography is more commonly used, but there may be a problem if one of the people loses the key. With asymmetric key encryption, the sender and receiver use different keys to encrypt and decrypt the data, but the keys are mathematically related. In most cases there is a private and a public key.

Just because data is encrypted does not mean the data is absolutely safe. There are people who try to decipher encrypted data. They sometimes use a brute-force attack, whereby the attacker attempts to use different keys on cyphertext and hopes that one changes the data into plain text.

A person who relies on cryptography to advocate for individual privacy is called a “cypherpunk.” Such individuals aim to accomplish increased privacy by using encryption and cryptography. Cypherpunks have been around for decades. A good summation of cypherpunk ideology can be found in Eric Hughes’s “Cypherpunk Manifesto” (1993). At their core, cypherpunks are concerned with maintaining an individual’s privacy as opposed to secrecy. As Hughes explains, secrecy is keeping information from everyone, whereas privacy is simply having the ability to choose whom to share information with and whom not to.

To foster a move toward cryptography-based systems of privacy, cypherpunks appear to have an open-source policy in regard to the codes they generate (Hughes, 1993). One of the items Hughes noted that cyberpunks were working toward was an electronic currency. In 2008, Satoshi Nakamoto started down this path by founding Bitcoin. The first Bitcoin transaction took place between Nakamoto and Hal Finney—a cypherpunk (Peterson, 2014). Bitcoin, as well as other cryptocurrencies, operate using blockchains that rely on cryptography.

See also: Bitcoin; Cryptocurrency; Nakamoto, Satoshi; Open-Source

Further Reading

Farrell, Henry. 2014. “The political science of cybersecurity II: Why cryptography is so important.” *The Washington Post*, February 12, 2014. https://www.washingtonpost.com/news/monkey-cage/wp/2014/02/12/the-political-science-of-cybersecurity-ii-why-cryptography-is-so-important/?utm_term=.6ab2bd6bd4bf

Hughes, Eric. 1993. “A cypherpunk’s manifesto.” https://www.activism.net/cypherpunk/manifesto.html

Martin, Keith M. 2017. *Everyday cryptography: Fundamental principles and applications*. Oxford: Oxford University Press.

Musa, Sarhan M. 2018. *Network security and cryptography: A self-teaching introduction*. Dulles, VA: Mercury Learning and Information.

Nakamoto, Satoshi. 2008. "Bitcoin: A peer-to-peer electronic cash system." Bitcoin.org. https://bitcoin.org/bitcoin.pdf

Peterson, Andrea. 2014. "Hal Finney received the first Bitcoin transaction. Here's how he describes it." *The Washington Post*, January 3, 2014. https://www.washingtonpost.com/news/ the-switch/wp/2014/01/03/hal-finney-received-the-first-bitcoin-transaction-heres-how-he-describes-it/?utm_term=.82ddd0bb27d8

Stallings, William. 2011. *Cryptography and network security: Principles and practice*, 5th Edition. Boston: Prentice Hall.

CYBERBULLYING

Cyberbullying can be defined in multiple ways, such as "actions using information and communication technology to harm another person" (Bauman, 2011, p. 4). Another similar definition explains bullying as being when a person is "tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted" (Stop cyberbullying, n.d.). In 2014, experts working with the Centers for Disease Control and Prevention, along with officials at the U.S. Department of Education, came up with a uniform definition of bullying: "Bullying is any unwanted aggressive behavior(s) by another youth or group of youths who are not siblings or current dating partners that involves an observed or perceived power imbalance and is repeated multiple times or is highly likely to be repeated." In short, cyberbullying is the use of technology or electronic devices to post messages or comments that are abusive or harassing or may cause the victim to feel ashamed or embarrassed. It may include embarrassing pictures or personal information or rumors that are defamatory. The hurtful behavior is intentional and repeated. It is also typically directed toward a person who is not able to, or lacks the power to, defend themselves (Patchin, 2017b).

Cyberbullying is not a single incident of an offensive comment. It is recurring negative comments and attacks that are aimed at one individual. These attacks can be very harmful to the victim, especially if they continue for a long period of time. Victims will often feel traumatized, and experience distress and anxiety. Some may also stop attending school (Patchin, 2017a). Cyberbullying can cause not only embarrassment to the victim but also, in some cases, physical harm. There have been many cases of people dying by suicide due to the effects of cyberbullying. Those who cyberbully another person may threaten to harm the victim, a family member, or friend.

The impact of cyberbullying can be grim. In 2002, Gyslain Raza, a teenage boy from Quebec, Canada, made a video of himself using a golf club to imitate the lightsaber action sequences seen in the *Star Wars* film franchise. Other students found the video in his high school's video studio and uploaded it to the internet without Raza's knowledge. The video was viewed over 900 million times and spawned a number of spoofs. Raza dropped out of school and had to receive therapy. He sued the four students who posted the original video. The case was settled out of court.

On September 9, 2013, 12-year-old Rebecca Sedwick killed herself by jumping off a silo. She had been bullied by other girls through social media postings and even moved to a different school but could not get away from the harassment, much of which was on social media. Two other girls, ages 12 and 14, were eventually arrested and charged with felony aggravated stalking for their behavior toward Rebecca.

Megan Meier's story was much the same. Megan, who was 13 and lived in Missouri, had been bullied for years in her school. Megan met a young man named Josh Evans on the social media site MySpace. The pair had pleasant conversations for about six months, and Megan thought Josh liked her. After that, Josh began writing negative messages to Megan, such as, "The world would be a better place without you" (Maag, 2007). Other people also began to post negative messages about Megan online. Even though Megan's mother told her to sign off, Megan chose to remain online and continue to read the messages. After reading the negative comments, Megan hanged herself in her closet.

In the end, there was no person named Josh. Lori Drew, the mother of Megan's classmate and former friend, wrote the comments that claimed to be from "Josh." Megan and Drew's daughter had a fight, and Drew formed a relationship with Megan under the false pretenses of being a teenage boy, as a way to find out what people were saying about her daughter. Drew also sought to embarrass Megan. After their conversations were becoming, as Drew described, tedious, she sought to end it and began writing negative comments. Drew was prosecuted under the Computer Fraud Act of 1986 that was intended to be used on hackers. She was convicted of three misdemeanor offenses, but the judge dismissed all charges against her. The events led members of Congress to propose the Megan Meier Cyberbullying Prevention Act in 2008 that would have made it a crime to coerce, intimidate, harass, or cause substantial emotional distress to a person (Hinduja and Patchin, 2013, p. 17). However, the proposed bill did not have enough support to pass.

Cyberbullying can take place in chat rooms, blogs, e-mails, texts, social networks (Twitter, MySpace, Instagram, Snapchat, or Facebook), YouTube, or any other online communication platform. It has even occurred on online gaming sites where players have online roles. Cyberbullying must involve at least one minor. If it involves only adults, it is considered to be cyberharassment or cyberstalking.

Bullying is an act that has existed for many years. Teasing between children or even adults is not a new phenomenon. However, it used to be a physical behavior and not concealed. If a person was bullied, the offender was known to them. Bullying behaviors today are an extension of traditional types of bullying. Comments made on social media are widely distributed. The number of people who can read the comments or who are exposed to them is huge. Many people make comments whether they know the victim or not. Moreover, those comments may remain anonymous, so they are sometimes very offensive, cruel, or hurtful.

According to the National Crime Victimization Survey, in 2015 about 20.8 percent of students admitted they were the victims of bullying. Much of today's cyberbullying behavior takes place in schools and among teenagers. In fact, most cyberbullying occurs in ninth and tenth grade (Englander, 2013). It is not uncommon as early as elementary school. School officials are usually trained to recognize bullying behavior, but it is difficult to stop. Even though teachers are trained, it can be difficult to remove messages from the internet once they have been posted and sent to others. It is also difficult to prevent further postings. There are multiple places where people can post comments, including the internet, social media, and phones, among others.

There are some other related terms to cyberbullying. In "flaming," or online fighting, people send angry messages, often obscene, to one another. These insulting interactions are often personal attacks and are often filled with untruths. They can be frustrating, annoying, and hurtful to everyone involved.

Another term is "masquerading," which occurs when a person pretends to be another person and sends messages or posts items that appear to come from the person. The postings may be false or embarrassing (whether true or false). A similar term is "outing," which is when confidential information is posted that can be embarrassing or hurtful. It is usually done to "out" a person by telling an embarrassing secret or posting embarrassing pictures. A more recent behavior, called "catfishing," occurs when a person presents false information to create a relationship with another person.

Trolling is a third related term. Trolling refers to the process of deliberately and secretly making people mad on the internet. This can be done by making random unsolicited and/or controversial comments or posts that serve to make others angry, possibly provoking an argument or fight. These are people who seek to cause trouble for no apparent reason. Those who seek to troll a victim will often make comments about YouTube videos, about blogs, or in forums. They also often make comments on social media sites. They may post misinformation or make a sarcastic remark simply to get a rise out of another user or start a fight. Some say that trolling is just pranks that are meant to simply poke fun at others, but others say that trolling amounts to online harassment by people who like to cause trouble.

A person who is found guilty of cyberbullying can be charged with harassment. New statutes have made cyberharassment a crime, but in some jurisdictions, cyberbullying behavior is a form of bullying in general. Many states have passed some form of legislation to deter cyberbullying, many of which require local schools to create antibullying policies. The effect of these policies may be limited, however, because much of the cyberbullying occurs during nonschool hours.

See also: Cyberstalking

Further Reading

Bauman, Sheri. 2011. *Cyberbullying: What counselors need to know*. Alexandria, VA: American Counseling Association.

Belsey, B. 2008. Definition of cyberbullying. www.cyberbullying.ca

Clough, Jonathan. 2015. *Principles of cybercrime*. Cambridge, UK: Cambridge University Press.

Englander, Elizabeth Kandel. 2013. *Bullying and cyberbullying: What every educator needs to know*. Cambridge, MA: Harvard Education Press.

Hinduja, S., and J. Patchin. 2013. Description of state cyberbullying laws and model policies. www.cyberbullying.us/Bulling_and_Cyberbullying_Laws.pdf.

Konnikova, Maria. 2015. "How the internet has changed bullying." *New Yorker*, October 21, 2015. http://www.newyorker.com/science/maria-konnikova/how-the-internet-has-changed-bullying

Maag, Christopher. 2007. "A hoax turned fatal draws anger but no charges." *New York Times*, November 28, 2007. https://www.nytimes.com/2007/11/28/us/28hoax.html

McQuade, Samuel C., III, James P. Colt, and Nancy B. B. Meyer. 2009. *Cyber Bullying: Protecting kids and adults from online bullies*. Westport, CT: Praeger.

Moreau, Elise. 2018. "Internet Trolling: How do you spot a real troll?" *Lifewire*, January 2, 2018. https://www.lifewire.com/what-is-internet-trolling-3485891

O'Neill, M. 1995. "The lure and addiction of life online." *New York Times*, March 8, 1995. http://find.galegroup.com/gtx/retrieve.do?contentsSet=IAC-Documents&resultListType=RESULT_LIST&qrySerId=Locale

Patchin, Justin W. 2017a. "Millions of students skip school each year because of bullying." Cyberbullying Research Center, January 3, 2017. http://cyberbullying.org/millions-students-skip-school-year-bullying

Patchin, Justin W. 2017b. "New bullying Data—and definition—from the National Crime Victimization Survey." Cyberbullying Research Center, January 13, 2017. http://cyberbullying.org/new-bullying-data-definition-national-crime-victimization -survey

Phillips, Whitney. 2015. *This is why we can't have nice things: Mapping the relationship between online trolling and mainstream culture*. Cambridge, MA: MIT Press.

Smith, P. K., J. Mahdavi, M. Carvalho, and N. Tippett. 2006. "An investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying: A report to the Anti Bullying Alliance." Brief No. RBX 03-06. Available at http://www.dcsf.gov.uk/research/data/uploadfiles/RBX03-06.pdf

Stein, Joel. 2016. "How trolls are ruining the internet." *Time*, August 18, 2016. http://time.com/4457110/internet-trolls/

Stop cyberbullying. n.d. http://www.stopcyberbullying.org/what_is_cyberbullying_exactly.html

CYBEREXTORTION, *see* RANSOMWARE

CYBERSECURITY

Cybersecurity refers to the procedures that are taken to protect computers, networks, and programs from a cyberattack or acts of cybercrime (e.g., viruses, malware, or ransomware). It is also referred to as information technology security. Most cyberattacks are carried out by offenders who are able to achieve unauthorized use of a computer system. They typically have the intent to harm a business, either directly or indirectly, by stealing data and information, ruining equipment or networks, or in some way causing damage to a business reputations or disrupt the lives of victims. Recent attacks on U.S. government sites have been traced to foreign governments. Cybersecurity is intended to prevent these attacks and protect against identity theft, malware, ransomware, the loss of money or other personal information. Cybersecurity helps a business or individual protect sensitive data (financial data, health care information, or trade secrets) from becoming public. Cybersecurity is necessary to protect businesses but also to protect governments (from digital spying), medical facilities, retail business, and even individuals and consumers (to protect their privacy, their financial status). This has become a fundamental part of most organizations' risk-management tasks.

The different forms of cybersecurity that are used as a way to prevent attacks are constantly changing, as the attacks and crimes carried out on them are constantly evolving. This means that as the forms of attack change, the response must also change. Cybersecurity can include numerous things, including technology or software. An effective method for ensure safety should include multiple techniques because an attacker may know how to evade one safety measure, but a second one may prevent the attacker from being successful.

One type of cybersecurity is software and technology that are intended to protect against malware such as viruses (antivirus protection) that can be unintentionally uploaded onto a computer through an e-mail or by visiting a fraudulent website. They can detect malware on e-mails or websites and can detect vulnerabilities in a system. Other software programs help to identify a threat or an attack that has been launched. These attacks need to be identified before they are able to progress too far. Other software that can be used by an organization to increase cybersecurity allows for the encryption of any data that is being sent electronically or being stored in the cloud. Firewalls can be installed to protect against unauthorized access to a computer system.

Cybersecurity can also be as simple as security training: educating employees about forms of social engineering intended to trick employees into providing passwords or private information which is the used to break into a network. Employees should be educated to choose secure, complex passwords and to keep them private. They should understand what phishing is and how it happens, and should be caution when opening e-mail attachments that are not from a known source. They should not go to websites that are not trusted. All data should be backed up regularly.

As a way to increase the nation's cybersecurity, the Federal Government passed the Cybersecurity and Infrastructure Security Agency Act of 2018, which replaced the former National Protection and Programs Directorate (NPPD) with the new agency, the Cybersecurity and Infrastructure Security Agency (CISA). CISA is the federal agency that is responsible for protecting the country's computer infrastructure. It focuses on combating cyberattacks and other forms of cybercrime by working to secure the federal computer networks and protect the country's critical infrastructure. CISA officials work alongside federal and state agencies as well as members of the private sector to provide increased tools to increase their cybersecurity efforts. CISA employees also provide incident response assistance in the case of a cyberattack.

In 2018, officials at the Corporate Finance Division of the Securities and Exchange Commission (SEC) issued new guidance on cybersecurity for companies. This includes more disclosures of risk oversight and disclosure of company controls and procedures regarding cybersecurity, among other things. If a cyberincident does occur, officials from the SEC will be permitted to investigate the event. One goal of the new policies is to ensure that all companies have cybersecurity policies in place, but another goal is to increase awareness of cybersecurity so any problems can be addressed.

Because of the critical need for increased cybersecurity, some experts have proposed a new cabinet-level department in the federal government that would oversee the country's cybersecurity. The agency would direct the government's cybersecurity policies to ensure a safer online environment for government, businesses, and individuals by reducing cyberthreats and attacks. Proponents of this idea argue that the development and administration of the nation's cybersecurity is currently spread among several different agencies, making it inefficient and sometimes ineffective. Others argue that an international framework for cybersecurity would be effective, especially for the banking industry. Supporters argue that international standards and norms to protect international property as well as online financial organizations should be developed to protect consumers and governments.

See also: Encryption; Identity Theft; Malware; Phishing

Further Reading

Burne, Katy. 2016. "BIS group creating guidelines for cybersecurity responsibility at banks, Swift." *Wall Street Journal*, September 15, 2016. https://www.wsj.com/articles/bis-group-creating-guidelines-for-cybersecurity-responsibility-at-banks-swift-1473966813

Clinton, Larry. 2015. Best practices for operating government-industry partnerships in cyber security. *Journal of Strategic Security* 8, 4: 53–68.

Shumsky, Tatyana. 2018. "SEC wants companies to boost cybersecurity, Brexit, Libor Phaseout Disclosures; Regulator wants companies to align policies with new cybersecurity disclosure guidance." *Wall Street Journal,* November 13, 2018. https://www.wsj.com/articles/sec-wants-companies-to-boost-cybersecurity-brexit-libor-phaseout-disclosures-1542142258

U.S. Department of Homeland Security. CISA. https://www.dhs.gov/CISA

U.S. Department of Homeland Security. "Cybersecurity." https://www.dhs.gov/topic/cybersecurity

Von Solms, Rossouw and Van Niekerk, Johan. 2013. From information security to cyber security. *Computers and Security* 38 (October): 97–102.

CYBERSECURITY ACT OF 2012

Senator Joe Lieberman (I-CT) introduced the Cybersecurity Act of 2012 (SB 2105) in February 2012, along with four cosponsors: Susan Collins (R-ME), Dianne Feinstein (D-CA), John Rockefeller (D-WV), and Sheldon Whitehouse (D-RI). The general purpose of the law was to enhance the cybersecurity of the nation's infrastructure as it pertains to national security, its economic security, or the nation's health and safety. The bill's supporters sought to increase security practices that would be cost-effective and efficient while at the same time protecting civil liberties of citizens and their right to privacy.

Under the proposed bill, the secretary of Homeland Security was given the responsibility to designate structures in the United States as a component of the nation's critical infrastructure. In order to be included, the structure would have to meet two requirements. First, the structure must be one that if it were incapacitated or disrupted, there would be a debilitating effect on national security, the nation's economic security, or the health or safety of the public. Second, the structure had to be dependent on information in order to operate. The secretary could also take other factors into consideration when designating structures as critical infrastructure, such as any interdependencies with other critical infrastructure components or the size of the structure.

Provisions in the proposed law encouraged all stakeholders to regularly discuss ways to increase national security through something called the Critical Infrastructure Partnership Advisory Council. This would include representatives from sector-specific agencies that oversee the country's critical infrastructure, agencies that regulate the critical infrastructure, those with specific expertise on services provided by the critical infrastructure, as well as those in the private sector who own or operate the critical infrastructure. Increased communication and exchange of information was highly encouraged. The proposed law defined "covered critical infrastructure" as any critical infrastructure that would be protected under the new law.

In addition to defining critical infrastructure, the secretary of Homeland Security was also given the task of establishing risk-based tiers that defined some infrastructure as more critical than others. These critical components would receive more protection than others. The tiers would have been based on the vulnerability to an attack, the ability of the infrastructure to survive a cyberattack, and the consequences if the infrastructure was attacked. This list would be reviewed and updated as necessary.

Under Section 4 of the proposed law, the secretary of Homeland Security was required to establish a process that would be used to identify cybersecurity risks that could be mitigated as a way to protect the nation's infrastructure. The secretary was to work with other agencies, state and local governments, and the private sector to develop these standards. In Section 5 of the proposed law, the owners or operators of critical infrastructure were asked to create plans to increase cybersecurity. They would also certify that the plans were being implemented.

Evaluations were part of Section 6 of the law. Here, the secretary was required to determine if the owners and operators of critical infrastructure were carrying out mitigation efforts. The secretary was to select an accreditor (evaluator) who would evaluate the critical infrastructure, monitor and inspect the operations of the infrastructure, and ensure that the infrastructure is complying with their mitigation plans.

All owners or operators of a critical infrastructure would be required to report any incident of concern to the secretary of Homeland Security. The secretary would then have been required to develop a plan to disseminate that information to the attorney general, who would promptly investigate it. However, under Section 7, the information is protected from public disclosure and exempted from publication under the Freedom of Information Act of 1967. Further, any security information could not be disclosed to the public. One exception to this provision allows for information to be shared with other government agencies to mitigate any further cybersecurity threats, or to assist other federal government agencies to carry out their functions. This provision was included to prevent others from exploiting any identified vulnerabilities.

Other provisions in the law would add other elements to protect the country's infrastructure. One provision amended the Homeland Security Act of 2002 to establish a National Center for Cybersecurity and Communications. The duties of the Center would be to manage efforts to secure, protect, and ensure the resiliency of the federal information infrastructure. Another provision required the secretary of Homeland Security to implement outreach and awareness programs on cybersecurity and to create a program to identify, develop, and recruit talented individuals to work in cybersecurity.

Agencies other than DHS would have been given additional responsibilities under the law. For example, the director of the National Science Foundation (NSF) was given the task of establishing a program that would increase innovation in cybersecurity research. They were also tasked with recruiting and developing professionals to work in the field of cybersecurity. Another agency, the Director of the Office of Personnel Management (OPM), was given the responsibility to assess the readiness of the federal agencies to meet cybersecurity needs. Along with this, they were to create an awareness and education curriculum for all federal employees and contractors about the need for cybersecurity.

A third agency that would have had additional tasks was the Department of Education. Officials here would have had to develop model curriculum for elementary students to increase their awareness of cybersecurity issues. Finally, the director of the Office of Science and Technology Policy was required to develop a national cybersecurity research and development plan that would have advanced the development of new technologies to protect the country's infrastructure against any threats of cybercrime. The bill received a lot of attention, but it did not have enough support to become law. The Senate vote on the bill was 52-46, preventing it from moving to the House of Representatives.

See also: CAN-SPAM Act of 2003; Computer Fraud and Abuse Act of 1986; Cybersecurity Enhancement Act of 2014; Cybersecurity Workforce Assessment Act of 2015

Further Reading

McCain, John, Kay Bailey Hutchison, and Saxby Chambliss. 2012. "No cybersecurity executive order, please." *Wall Street Journal*, September 13, 2012. https://www.wsj.com/articles/SB10000872396390444017504577647131630683076

S. 2105 (112th Congress): "Cybersecurity Act of 2012." govtrack. https://www.govtrack.us/congress/bills/112/s2105

"Section by section, cybersecurity regulatory framework for covered critical infrastructure." https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters

/cybersecurity-regulatory-framework-for-covered-critical-infrastructure-act-section-by-section-analysis.pdf

Shackelford, Scott J. 2011–2012. "In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012." *Stanford Law Review Online* 64: 106–111.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)

On November 16, 2018, President Donald Trump signed the Cybersecurity and Infrastructure Security Agency Act that established the Cybersecurity and Infrastructure Security Agency (CISA). The new agency oversees the nation's computer systems and acts as the country's risk advisor. It coordinates with businesses and other partners to protect computer networks against potential threats. It is responsible for ensuring that the country's computers secure and resilient in an attack should occur. The agency's mission statement is "Defend Today, Secure Tomorrow."

CISA provides information to agencies, businesses, and other stakeholders regarding cybersecurity. The agency's priorities include protection of the federal computer network, comprehensive protection of all computers, increasing the resilience of computer infrastructure, and increased emergency communications. The agency was assigned to provide information and alert agencies about any current threats that may impact systems. This includes information on possible patches, if needed, to help prevent the progression of an attack. Information will also be provided to the public so they are made aware of potential malware that could affect their computers. If needed, CISA will carry out detailed analysis reports on incidents. All information will be shared with all interested parties in a timely fashion.

Additionally, CISA serves as the federal government's agency to receive and process information on all cyber threats to the United States, including all federal and nonfederal agencies. Any information about a cyberincident will be exempt from public disclosure and will be protected from use in any potential civil litigation.

Included within CISA is the National Cybersecurity and Communications Integration Center (NCCIC). This organization comprises of the U.S. Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). The U.S. Computer Emergency Readiness, or U.S. CERT, was created in 2003 after Congress passed the Federal Computer Incident Response Center (FedCIRC). The agency was given the responsibility of analyzing and reducing cyberthreats across the United States. It provides information about security threats to stakeholders along with suggestions for avoiding them. Officials often work with experts from around the world to prevent cyberattacks. They provide cybersecurity protection to federal agencies as well as to state, local, tribal, and territorial governments. They are also tasked with responding to any incidents that may occur. ICS-CERT seeks to reduce the risk of a cyberevent within all critical infrastructure sectors. They work in conjunction with local law enforcement officials and private owners and operators on security issues and efforts for mitigation.

See also: Comprehensive National Cybersecurity Initiative; Cybersecurity

Further Reading

"Does the U.S. need a cabinet-level Department of Cybersecurity?" June 3, 2019. *Wall Street Journal*. https://www.wsj.com/articles/does-the-u-s-need-a-cabinet-level-department-of-cybersecurity-11559586996

Marks, Joseph. 2019. "The Cybersecurity 202: Trump's efforts failed to make critical infrastructure safer from cyberattacks, experts say." *The Washington Post*, March 5, 2019. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/03/05/the-cybersecurity-202-trump-s-efforts-failed-to-make-critical-infrastructure-safer-from-cyberattacks-experts-say/5c7d6c5b1b326b2d177d5fbd/?noredirect=on&utm_term=.45b2ab9bda35

McKinnon, John D. 2017. "Trump signs executive order aimed at protecting U.S. infrastructure, Homeland Security." *The Wall Street Journal*, May 11, 2017. https://www.wsj.com/articles/trump-signs-executive-order-aimed-at-protecting-u-s-infrastructure-homeland-security-1494527015

Trump, Donald J. 2017. "Executive order 13800—Strengthening the cybersecurity of federal networks and critical infrastructure." The American Presidency Project, May 11, 2017. https://www.presidency.ucsb.edu/node/327121

"The unreadiness team; Homeland Security's cyber-defense unit has done little in seven years." *The Washington Post*, June 20, 2010. https://www.pressreader.com/

CYBERSECURITY ENHANCEMENT ACT OF 2014

Senator John D. Rockefeller IV (D-WV) introduced the Cybersecurity Enhancement Act of 2014 to the Senate in July 2014. The law was intended to create a continuing, voluntary partnership between public and private agencies and individuals as a way to improve the nation's cybersecurity. There were also provisions in the law geared toward strengthening research and development in the cybersecurity area. Other areas of the bill were included to establish programs workforce development programs, education programs, and public awareness. The Senate and House of Representatives passed the bill on December 11, 2014. President Barack Obama signed the bill into law on December 18, 2014.

Title 1, Public-Private Collaboration on Cybersecurity aimed to facilitate the development of a voluntary federal plan to reduce the risks of cybercrime to critical infrastructure. The secretary of commerce was directed to oversee the development of the cybersecurity research and development strategic plan that was to set standards that would reduce risks of cybercrime to critical infrastructure across the country. The program was to be industry-led so that the plans would be workable and supported by all involved.

Under the law, the secretary, industry representatives, and private-sector personnel (critical infrastructure owners and operators) were to meet on a regular basis to help identify, assess, and manage cyber risks. Upon doing that, the participants were asked to identify possible impacts of the proposed measures on business owners' needs to keep much of the information involved confidential. Representatives from businesses were concerned about the possibility that they would be forced into making their business secrets public or releasing confidential security measures used in their facilities. For them, the law required that the group consider different methods to mitigate the potential impact that the new policies would have on these organizations.

At the same time, as the law noted, it was important to maintain the civil liberties and privacy of individuals, whether they be clients, customers, owners, or employees. The ultimate goal was to identify a prioritized, and flexible set of standards that were cost-effective and would be voluntarily adopted and supported by all involved.

Title 2, Cybersecurity Research and Development, stipulated that once the overall plan was developed, the heads of federal agencies and departments, along with owners and operators of critical infrastructure, would meet every four years to update it. This would keep it relevant to any new technology. The research and development strategy included 10 federal agencies, including the Department of Defense, the NASA, the Department of Energy, and the Environmental Protection Agency (EPA), among others.

Title 3, Education and Workforce Development, supported internships or other work experience in the federal government through scholarships. The director of the National Science Foundation, along with the director of the Office of Personnel Management and the Secretary of Homeland Security, were charged with overseeing the Federal Cyber Scholarship for Service Program. This was to provide scholarships to college students who are interested in careers in cybersecurity. This would help to train the next generation of information technology professionals. The law mandated that any student who received the scholarship would be required to work in the period equal to the length of the scholarship.

In Title 4, Congress created the National Cybersecurity Awareness and Education Program. The director of the National Institute of Standards and Technology was asked to coordinate a national cybersecurity awareness and education program for the public that would increase the general awareness of cybersecurity, online safety, and cyberethics.

The final part of the law, Title 5, was labeled Advancement of Cybersecurity Technical Standards. Here, it was required that there be coordination with all federal agencies and that they be included in the development of international standards related to cybersecurity.

See also: CAN-SPAM Act of 2003; Cybersecurity Act of 2012; Cybersecurity Workforce Assessment Act of 2015

Further Reading

Benzel, T. 2015. "A strategic plan for cybersecurity research and development." IEEE Security & Privacy 13. https://ieeexplore.ieee.org/abstract/document/7180232/

Rodin, Deborah Norris. 2014–2015. "The cybersecurity partnership: A proposal for cyberthreat information sharing between contractors and the federal government." *Public Contract Law Journal* 44: 505.

S.1353—Cybersecurity enhancement act of 2014. Congress.gov. https://www.congress.gov/bill/113th-congress/senate-bill/1353

CYBERSECURITY WORKFORCE ASSESSMENT ACT OF 2015

As part of the Consolidated Appropriations Act of 2016, the Cybersecurity Workforce Assessment Act aimed to protect the nation's information technology systems and networks and protect sensitive data. This would also help to protect the financial, health care, transportation, and energy grids for the nation. It was also meant to attract a diverse pool of applicants to fill cybersecurity-related openings. President Barack Obama signed the bill into law on December 18, 2015.

The law had two goals: to increase and improve the workforce in federal cybersecurity positions in the DHS by providing education and training to employees who require it and to increase collaboration between federal agencies, the Office of Personnel Management, and the National Initiative for Cybersecurity Education in order to reduce cybercrime.

To improve the federal workforce in cybersecurity, the law directs the secretary of Homeland Security to carry out a review of the cybersecurity workforce in the department within 180 days of the bill's passage. The assessment includes the readiness and capacity of the DHS workforce to meet its cybersecurity mission; the location of cybersecurity workforce positions within DHS; which tasks are performed by permanent full-time employees, by independent contractors, or by individuals who are employed by other federal agencies; which positions are vacant; the percentage of individuals within each specialty area who have received essential training necessary so they can perform their jobs effectively; and, in cases where training was not received, what challenges were encountered regarding the training.

Once this is done, the secretary is to develop and then implement a strategy to maintain a workforce that is trained, ready, and capable of preventing cybercrime. Moreover, every three years, the secretary must update the strategy to include a plan to recruit qualified personnel, a 10-year projection of the cybersecurity workforce needs of DHS, and a list of potential obstacles to reaching that goal. The project should also include an indication of any gaps that may exist in the workforce at DHS and a plan to fill that gap.

The law provides for scholarships and tuition waivers for many employees seeking additional education or training needed to more effectively perform their jobs. The agency also works with colleges and universities who offer a cybersecurity curriculum to support employee education and training. The law also allowed DHS to recruit additional employees as needed, hire new employees who have cyber skills, and retain those employees who already have the skills needed to perform the tasks. The law also enables DHS to hire new employees as needed to address new cybercrimes as they evolve.

To reach the second goal of increasing collaboration between agencies, the law mandates that the agencies involved come up with a better way to share information about cybersecurity with private-sector agencies and federal government agencies. This way, information on possible cybersecurity threats can be more easily shared with other agencies. The law also establishes a system for government agencies and private agencies to monitor particular information systems to stop cyberattacks. This can be done with the help of the National Cybersecurity and Communications Integration Center, which is part of the Department of Homeland Security, which will serve as a clearinghouse for information. Any private agencies that choose to share information will not be forced into providing any information that may result in the loss of trade secrets. They will also be protected from any liability.

The law will be effective for 10 years after its effective date unless Congress opts to change it or pass another piece of legislation.

See also: CAN-SPAM Act of 2003; Cybersecurity Act of 2012; Cybersecurity Enhancement Act of 2014

Further Reading

Cobert, Beth. 2016. "Strengthening the federal cybersecurity workforce." U.S. Office of Personnel Management. July 12, 2016. https://www.opm.gov/blogs/Director/2016/7/12/Strengthening-the-Federal-Cybersecurity-Workforce

Evangelakos, John, Brent J. McIntosh, Jennifer L. Sutton, Corey Omer, and Laura S. Duncan. 2015. "A guide to the Cybersecurity Act of 2015." Law 360, January 12, 2015. https://www.law360.com/articles/745523/a-guide-to-the-cybersecurity-act-of-2015

HR 2952. "Cybersecurity workforce assessment act." Congress.Gov. https://www.congress/gov/bill/113th-congress/house-bill/2952/text.

6 USC 146: "Cybersecurity workforce assessment and strategy." https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title6-section146)&num=0&edition=prelim

CYBERSQUATTING

Cybersquatting is the practice of claiming a domain name that is likely to be sought by another entity (usually a corporation) with the intent of selling that domain name to that entity at a price significantly higher than what it was initially purchased for. In the United States, this practice is illegal under the Anticybersquatting Consumer Protection Act (15 U.S. Code § 1125(d)), which was enacted on November 29, 1999. Those found in violation of this law are not guilty of a crime (e.g., they would not be subject to criminal penalties such as incarceration). Rather, those who violate the law can be sued in a civil cause of action by the person whose domain name was wrongfully squatted on by the offender. If the court finds the offender did in fact squat on a domain name in bad faith (e.g., with the intent to adversely affect the person who filed the complaint), the court may order the domain name be transferred from the offender to the person who filed the complaint, or that the domain name be canceled.

Internationally, claims of cybersquatting can be handled by the World Intellectual Property Organization's (WIPO) Arbitration and Mediation Center. In 2017 alone, the organization handled over 3,000 cases of cybersquatting (World Intellectual Property Organization, 2018). Arbitration and mediation are methods by which a case can be resolved without formally filing a complaint in court. This generally requires both parties to agree to resolve the case through arbitration or mediation. This is technically the case with arbitration and mediation through WIPO. However, when someone registers a generic top-level domain name (gTLD)—a domain name ending with a recognized top-level domain designation such as .com, .net, or .org—they are required as part of the terms and conditions to agree to resolve disputes over that domain name through arbitration and mediation with WIPO. The decisions of WIPO are binding in as much as accredited companies that register domain names must undertake actions to comply with arbitration and mediation orders from WIPO—namely transferring domain names from the offending party to the party wronged. However, the decisions made by WIPO are not binding on a court of law, and thus if one party or the other decides to initiate court proceedings over a domain name dispute, WIPO may terminate arbitration and mediation proceedings.

One example of cybersquatting is the case *Virtual Works, Inc. v. Volkswagen of America*, 238 F.3d 264 (2001). In that case, Virtual Works registered the domain name vw.net, with the knowledge that Volkswagen may one day want to own that domain name. Volkswagen ultimately did contact Virtual Works about buying the domain name. Through Volkswagen's communications with Virtual Works, it believed that Virtual Works was operating in bad faith. Volkswagen ultimately pursued legal recourse, and the courts ultimately held Virtual Works in violation of cybersquatting laws.

Another example of cybersquatting is that of *People for the Ethical Treatment of Animals v. Doughney*, 263 F.3d 359 (2001). In that case, Michael Doughney registered the domain name peta.org. Doughney called the website "People Eating Tasty Animals." There was some indication that Doughney was looking to gain financially from this transaction. The court ultimately ruled against Doughney.

The practice of cybersquatting has extended to the realm of social media. Cybersquatters will claim profile names that belong to celebrities and companies. Federal cybersquatting law specifically applies to domain names. However, social media sites will often have prohibitions against name squatting or similar behavior in their terms of use. Twitter will generally suspend the account of someone who infringes on the trademark of someone else, and will permanently suspend the account of someone who attempts to get money in exchange for a username (Twitter, 2018). Facebook and Instagram have rules prohibit the use of usernames that imitate someone else and infringing on trademarks respectively, but neither indicate what the punishment for violating those rules is (Facebook, 2018; Instagram, 2018).

This notwithstanding, it appears some social media users may have found a way to informally deal with the cybersquatting situation. Some celebrities have taken to adding the word "real" somewhere in their Twitter handle to indicate their account is the one that actually belongs to them, which also alleviates the need to deal with a cybersquatter who registered an account that is simply their name. Examples include comedian Kevin Hart (@KevinHart4Real), actor Hugh Jackman (@RealHughJackman), and President Donald Trump (@realDonaldTrump).

A practice similar to cybersquatting is typosquatting. Typosquatting is the act of purchasing a domain name with a spelling that is slightly off from a popular domain name. An example of typosquatting is the case *Lamparello v. Falwell*, 420 F.3d 309 (2005). In that case, Christopher Lamparello, after hearing Reverend Jerry Falwell share views on homosexuals that Lamparello found objectionable, registered the site www.fallwell.com, a domain name that included one more "L" than Falwell's www.falwell.com. Lamparello used his site to combat what he saw as falsehoods that Falwell was teaching about LGBTQ persons. The court ruled in Lamparello's favor as he did not appear to be using the site to elicit money from Falwell.

In another case, a Canadian teenager named Mike Rowe registered the domain name mikerowesoft.com, a play on his name. Lawyers for Microsoft in Canada contacted Rowe and informed him they believed his website infringed on Microsoft's trademark. The matter was ultimately settled out of court with Rowe receiving, among other things, an Xbox (Kotadia, 2004).

While typosquatting can be used in the same way as cybersquatting to elicit money from the individual or corporation whose domain name is being mimicked, it can also be used as a means of driving more unintentional web traffic to a site. This practice, per se, does not appear to be illegal in the United States.

See also: Social Media

Further Reading

Facebook. 2018. "Your Facebook web address." https://www.facebook.com/help/usernames

Instagram. 2018. "What if an account is using my registered trademark as its username?" https://help.instagram.com/101826856646059

Kotadia, Munir. 2004, January 26. "MikeRoweSoft settles for an Xbox." *CNet*. https://www.cnet.com/news/mikerowesoft-settles-for-an-xbox/

Twitter. 2018. "Username squatting policy." https://help.twitter.com/en/rules-and-policies/twitter-username-squatting

World Intellectual Property Organization. 2018. "WIPO cybersquatting cases reach new record in 2017." http://www.wipo.int/pressroom/en/articles/2018/article_0001.html

CYBERSTALKING

Cyberstalking is the stalking of another person that is carried out through an online format. A similar term, cyberharassment, involves posting offensive messages about another person online. Both involve the use of technology (e-mail or social media) to repeatedly harass or perform surveillance techniques on another person that may continue for several months or even years. It is an extension of traditional, physical stalking and is a relatively new crime that has evolved as new technology has evolved. Cyberstalking and cyberharassment both include some kind of communication with the victim; publishing information about them (sometimes "outing" them); watching (or stalking) the victim; publication of false information; or disclosure of true information that could be very embarrassing.

Some people use the terms stalking and harassment interchangeably, but there is a distinction between the two terms. Harassment can be annoying behavior that is bothersome but usually not harmful, either emotionally or physically. Stalking occurs when this behavior becomes hurtful, threatening, or dangerous, or when it causes a reasonable person to be fearful. Cyberstalking is also different from trolling, which is behavior that is not intended to cause harm and usually involves some humor. A cyberstalker typically has malicious intent. A new type of cyberstalking is catfishing, which occurs when the stalker pretends to be someone else. They will use fake identification, fake name, and photos, or pretend to be a mutual friend of the victim, or even an admirer. Another related behavior is flaming, which is online verbal abuse. Doxing occurs when someone gathers identifiable personal information about another person as a way to defame, scare or blackmail them. They may want to embarrass them, or extort them.

A victim of cyberstalking may feel frightened or threatened, especially if the attack happens over a period of time. A victim does not know when the person will appear next or what they will do next. The information posted by a stalker may be damaging to a victim's reputation, and if severe enough, can harm their career. In some cases, the victim is actually harmed physically, sometimes resulting in death. Some victims suffer from emotional victimization if the offender posts embarrassing information about them, whether true or not. Victims can feel helpless, and may become distrustful of others. Physical effects that victims often report experiencing include headaches, panic attacks, anxiety, loss of sleep, PTSD, and social withdrawal. Many victims experience psychological effects as well.

The National Institute of Justice created the Model Anti-Stalking Code, which defines stalking as a "course of conduct that is directed at a particular person that often causes the victim to experience fear of injury or death." Under the model code, the offender must know, or should know, that their conduct will create fear in the victim. This code is intended to serve as a model piece of legislation for states to emulate as they create their own anti-stalking laws (Baum, Catalano, Rand and Rose, 2009).

There are many ways to pursue another person online. A stalker may post personal information online that can be embarrassing to the victim, such as e-mails that have been hacked. That posted information may often be false but yet convincing to an outsider, thereby not only causing embarrassment but also potentially ruining their reputation. A stalker can sexually harass the victim by sending and posting pornographic, violent, or offensive photos or videos. Another method commonly used by stalkers is to make threats not only against the individual but also against other family members. Offenders have been known to track a victim's movements, call, e-mail, or text them an excessive number of times each day or hack into a victim's e-mails and then use them to harass the victim or blackmail them. Some stalkers will create a website that they use to harass the victim. The stalker can post messages that include the victim's phone number or e-mail address and ask others send threatening messages to the victim. In some cases, offenders have placed orders for goods and services, such as subscriptions to pornographic magazines, expensive goods, or excessive amounts of a product. These can be delivered to a victim's place of employment, bringing further embarrassment.

In the past, traditional or offline stalking required the victim and offender to be in the same geographical area. Today, a cyberstalker can be physically located anywhere, and they do not need to confront the victim. This means that the social barriers to harassing another person no longer exist. Moreover, a cyberstalker may never be identified, and most know they will not be caught and punished. This all makes it easier for an offender to stalk another.

Victims of cyberstalking don't always know the offenders. Men are more often the stalkers, and women are more often the victims (Kremling and Parker, 2018). The U.S. Department of Justice reports that 850,000 American adults, most of whom are women, are the victims of cyberstalking. In addition, the Pew Research Center indicates that 40 percent of adult internet users have experienced harassment online (Sweeney, 2014). The stalkers are often motivated by jealousy or revenge. An offender can also encourage other people to harass the victim, either in addition to his or her postings or in place of them. In some cases, the cyberstalker may arrange to meet the victim, sometimes leading to physical assault.

One organization that has the goal of reducing cases of online stalking is WHOA, or Working to Halt Online Abuse. They and other experts have suggested a number of ways to prevent cyberstalking. Some of the ideas are listed below:

1. Be sure to log out of your computer when you are done using it. This way no one will be able to use your account to send e-mails under your name or steal information that you may have left on the computer. Similarly, use passwords on cell phones so no one else has access to steal your information.
2. Be very clear to a potential stalker that their communication is unwanted. After that, have no further contact or communication with that person.
3. Use strong passwords, and don't give them out to anyone. Be sure to change passwords often.
4. Communicate online only with people that you know and trust. If you must communicate with strangers, set up an anonymous account for that.
5. Be careful of posting upcoming events you are attending, or even your calendar, on social media. A stalker could use this information to show up at events or track your comings and goings.
6. Be careful what private information is posted on social networks. Be sure to use privacy settings and limit who can view your information. Never provide any private information online. Remove any personal information that may currently exist and do not replace it.
7. Report any cyberstalking behavior to the police or to your internet service provider (ISP). If there are any hard copies of messages or communications, keep those in case you will need them as evidence.
8. Don't use a public Wi-Fi spot for personal e-mails or messages.
9. Maintain a current virus protection software on all computers or devices.
10. Don't upload photos that can show your location or places.

On the federal level, there is limited protection for victims. The Violence against Women Act (2000) included cyberstalking as part of the federal stalking statute. Another piece of legislation designed to protect victims of cyberstalking is the Combat Online Predators Act, authored by House member Brian Fitzpatrick (R-PA), a former FBI special agent and federal prosecutor. The purpose of the proposal was to increase criminal penalties for up to five years for behaviors related to the stalking of minors. The bill passed the House of Representatives but went no further. The proposal was in response to the cyberstalking of a female teen by a friend's 51-year-old father on social media. The father plead guilty to a misdemeanor stalking charge, and the judge in the case sentenced him to a term of probation and counseling. Three years later, in 2016, the same man contacted the female again. This time, he was arrested and sentenced to prison for a term of 18 months to seven years. The bill was proposed in 2017, but it did not have the support to be passed into law.

Some states have laws that ban harassing another person through electronic means, and others have included it in their general laws against stalking. Most of the state laws are vague and sometimes not effective in protecting victims. For example, California passed the first cyberstalking legislation in 1999, and the first person charged was Gary Dellapenta. This offender posted ads and responded to e-mails about rape fantasies using a woman's name. Men responding to the ads showed up at her apartment. Dellapenta was convicted and sentenced to six years in prison. In New York, Ian Barber posted nude pictures of his ex-girlfriend on Twitter and sent the pictures to her sister and employer; he was charged with three offenses, including aggravated harassment in the second degree. However, the charges were eventually dropped by prosecutors because the offender, Barber, did not send the pictures directly to the victim, an element required under the state law. In New Jersey, it is a criminal invasion of privacy to disclose sexual images without a person's consent.

A related term is flaming, which occurs when insults are exchanged in a chat room or other social media public setting. Examples of this can include rumors, lies, or other falsehoods, or even abusive or embarrassing posts.

See also: Craigslist Killers; Cyberbullying

Further Reading

Baum, Katrina, Shannan Catalano, Michael Rand, and Kristina Rose. 2009. Stalking victimization in the United States. Bureau of Justice Special Report, NCJ 224527. https://www.justice.gov/sites/default/files/ovw/legacy/2012/08/15/bjs-stalking-rpt.pdf

Bocij, Paul. 2004. *Cyberstalking: Harassment in the internet age and how to protect your family.* Westport, CT: Praeger.

Clough, Jonathan. 2015. *Principles of cybercrime.* Cambridge, UK: Cambridge University Press.

Hazelwood, S. D., and Sarah Koon-Magnin. 2013. "Cyber stalking and cyber harassment legislation in the United States: A qualitative analysis." *International Journal of Cyber Criminology* 7, 3: 155–168.

Kremling, Janine and Amanda M. Sharp Parker. 2018. *Cyberspace, cybersecurity, and cybercrime*. Thousand Oaks, CA: Sage.

Mullen, P. E., M. Pathe, and R. Purcell. 2009. *Stalkers and their victims.* New York: Cambridge University Press.

Paganini, Pierluigi. 2017. "Trolling, doxing & cyberstalking: Cybercrime & the law." Security Affairs. March 3, 2017. https://securityaffairs.co/wordpress/56841/laws-and-regulations/trolling-doxing-cyberstalking-cybercrime-law.html

Sweeney, Marlisse Silver. 2014. "What the law can (and can't) do about online harassment." *The Atlantic*. November 12, 2014. https://www.theatlantic.com/technology/archive/2014/11/what-the-law-can-and-cant-do-about-online-harassment/382638

CYBER-SURVEILLANCE MALWARE

Malware can be used as a way to spy on another person, group, or government. If the malware program can be successfully inserted into another's computer system, the program can gather information from the infected computer and send it back to the people or person who launched it, or it can be used to cause harm to the infected computer by damaging the equipment in some way. Three related malware programs were used in this way: Duqu, Flame, and Gauss. All three had the same characteristics and are assumed to be written by the same group, and all actively gathered information on the infected computer systems for months before detected.

Duqu Malware

The Duqu malware was also a form of cyberespionage that was not meant to cause harm to networks, but instead allowed the originators to gather information on the infected computer and send it back to the originator. Duqu was found mostly in the Middle East but also in India, Africa, and Eastern Europe, and most agree that it was written by government officials because of its complexity.

The virus contained a keylogger that stole information on all keystrokes made on the computer. It also saved screenshots and relayed those images back. The malware was discovered by experts in Budapest, Hungary, in September 2011. It seemed to "go dark" in 2012 but re-emerged in 2018 when it was used against Kapersky labs (a computer security firm) and other companies. This time it was referred to as Duqu 2.

The original virus was designed to allow the originator to collect intelligence data from different groups including industrial control manufacturers. Once the originators had the required passwords and credentials, they could then use that information to launch an attack sometime in the future without being detected. They may be able then to take control of an organizations computer systems to launch an attack that would in turn allow them to control the machinery in the factory. Many experts warned that Duqu should not be considered by most to be a threat to their networks, but it could be an indication of increased cyberwarfare between different governments, and possibly more harmful attacks.

Computer experts who studied the Duqu virus realized that it is much like the Stuxnet virus used against Iranian nuclear facilities. For that reason, Duqu is sometimes referred to as Stuxnet Jr. The Duqu virus has software rules that are virtually the same as those in Stuxnet, as well as the source codes and encryption keys. The only difference is the Duqu is more advanced. For those reasons, most people agree that Duqu and Stuxnet were written by the same people.

Flame Malware

Flame was the name of malware that was discovered in 2012. It was used to attack approximately 1,000 computers owned by governments, educational agencies, and private computers located in mostly in Iran, but the malware infected computers in Israel, Palestine, and other Middle Eastern countries as well as in Russia, Hong Kong, and Austria. The infected computers were running on Microsoft Windows operating system.

The Flame virus was used to collect sensitive information on the user. It allowed the developers to listen to Skype conversations, record audio, take screenshots, record keyboard strokes (to collect user names and passwords), and track internet searches. Once the information was collected, it sent it back to the person who was responsible.

It was alleged that the malware was a cyberweapon that was developed by the U.S. National Security Agency (NSA), the CIA, and military experts located in Israel. It was thought to be part of Operation Olympic Games, an effort to attack Iran's nuclear plants and gather information on their nuclear program. As such, it was very similar to the Stuxnet malware that was used in that operation. Investigators are unsure how the malware was originally put into machines, but once it was uploaded onto one computer, the virus would spread to others. It was also thought to infect a USB stick that was placed into a machine, and then upload from that device onto another computer.

The malware was difficult for victims to detect. It included a "suicide" command that would initiate after a period of time, or upon the command of the originator, and would remove the program from the computer, leaving no indication that it had been placed there. For that reason, many of the victims were unaware that their computers had been affected. The virus was discovered by experts at Kapersky labs after the United Nations International Telecommunications Union asked experts at the lab to investigate allegations that computers in the Iranian National Oil company had been attacked with malware. Upon its discovery, Iran's National Computer Emergency Response Team distributed a removal tool to agencies whose computers were infected.

Gauss Malware

Gauss was a cybersurveillance operation that was launched in September 2011 and discovered in June 2012 by the International Telecommunication Union (ITU), a group that works to promote online peace. They were investigating the Flame virus and discovered this variation of the malware. It is also thought to be related to the Duqu virus because it has the same general characteristics. The malware was named after Johann Carl Friedrich Gauss, a German mathematician.

Gauss is a state-sponsored malware that is based on the Flame platform. It was used to target foreign governments and intended to steal sensitive information from computers such as banking passwords, social media information, network interfaces, the content of computer systems, data, and account information. The malware gathers the sensitive information and then transmits it back to the people who launched it. Most infected computers were running the Windows 7 operating system.

Similar to the Flame virus, experts do not know how computers are originally infected with the Gauss malware but it is spread through an infected USB drive. The Gauss virus is not a self-replicating virus. The virus is known to have infected over 2,500 computers, but experts believe it actually affected more than that. It was launched on banking institutions located in the Middle East, primarily in Lebanon, but it was also found in Germany, Egypt, and the United States. The malware was written so that after a certain period of time, it removes itself from an infected computer, making it difficult to identify. The malware could also lie dormant in servers for many months, making detection more difficult. However, the virus uploaded a new font, Palida Narrow, so if a computer had the new font, it likely also had the virus.

The Gauss virus contains an encrypted module called Godel. It is unknown what purpose this was intended for.

See also: Encryption; Malware; Operation Olympic Games

Further Reading

Bencsath, Boldizsar, Gabor Pek, Levente Buttyan, and Mark Feleghazi. 2012. The cousins of Stuxnet: Duqu, Flame and Gauss. *Future Internet* 4: 971–1003.

Erdbrink, Thomas. 2012. “Iran confirms attack by virus that collects information.” *The New York Times*, May 29, 2012. https://www.nytimes.com/2012/05/30/world/middleeast/iran-confirms-cyber-attack-by-new-virus-called-flame.html

Nakashima, Ellen, Greg Miller, and Julie Tate. 2012. “U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say.” *The Washington Post*, June 19, 2012. https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html?noredirect=on

Rashid, Fahmida Y. 2012. Gauss attack toolkit targeting Lebanese banks related to Stuxnet, Flame. *Security Week*, August 9, 2012.

Storm, Darlene. 2012. “Gauss malware: Nation-state cyber-espionage banking Trojan related to Flame, Stuxnet.” Computerworld, August 9, 2012. https://www.computerworld.com/article/2597456/gauss-malware--nation-state-cyber-espionage-banking-trojan-related-to-flame--stuxnet.html

Zetter, Kim. 2012. “Meet ‘Flame,’ the massive spy malware infiltrating Iranian computers.” Security, May 28, 2012. https://www.wired.com/2012/05/flame/

CYBERTERRORISM

The word "cyberterrorism" is a vague term with multiple meanings, largely because of differences in cultural norms and religious ideologies that exist between countries. The word itself is a combination of the words "cyberspace" and "terrorism." Cyberterrorism (sometimes also called electronic terrorism) refers to large-scale acts of terrorism that take place by the use of the internet, or the threats of such acts by terrorists who rely on technology. Acts of cyberterrorism are intentional acts, committed through the use of a computer or other type of communication system, that are typically inspired by religious, political, or ideological reasons. These acts are geared toward harming information or data held on computers, or toward harming the computer systems, networks, or programs themselves through the use of malware or viruses. They are carried out against individuals, private companies, banks, and/or the government (especially the military). The goal of the cyberterrorist acts is to cause fear, destruction, or severe harm to populations, even death (Brenner, 2008), and to ultimately cause change through violence. It often results in a loss of revenue and release of the private information of the company or organization's employees. These acts do not include hacking into a website to change or alter it, which would be an act of cybervandalism.

The FBI defines cyberterrorism as "(t)he premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub-national groups or clandestine agents" (Singer, 2012). Another definition of cyberterrorism is provided by the U.S. National Infrastructure Protection Center, which is now part of the U.S. Department of Homeland Security (DHS). They characterize it as a "criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to particular political, social or ideological agenda" (Akhgar et al., 2014).

Dorothy Denning from Georgetown University provided a more detailed description of cyberterrorism in her testimony before the Special Oversight Panel on Terrorism of the Committee on Armed Services for the U.S. House of Representatives on May 23, 2000. She defined cyberterrorism as "the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not" (Denning, 2000).

A related term is cyberwarfare, which refers to events in which actors attempt to, or threaten to, sabotage a country's military and/or critical infrastructure. The goal is to threaten lives and ultimately create fear in the citizenry. The infrastructure refers to the financial institutions, water systems, communication systems and power grids that are essential to any community, city, state or nation. Examples include acts in which governments use the computer to spy on military communications of another nation; disrupt a website and services that result in inconvenience to customers, including situations could lead to death; and prevent people from accessing a website belonging to an organization or group that they disagree with. An example of this is the Stuxnet virus that was used by the United States to disrupt nuclear operations in Iran.

As with any act of cybercrime, an act of cyberterrorism is sometimes difficult to trace. These acts can be carried out anonymously and from far away from the site of the attack. An incident directed toward the United States. could be based in a country far away, even on the other side of the world. Moreover, an attacker may place false clues within the attack so the blame is placed elsewhere. Because of this, it is sometimes difficult to know the exact source of the attack or where to place blame.

Terrorists often rely on technology for a variety of acts. First, they use the internet to recruit new members and then encourage their members to carry out attacks. They use the internet to communicate with members. They raise funds to subsidize events. They can then use the internet to organize those attacks. They are able to circulate orders and coordinate supplies. Second, they use the internet for propaganda. They can attempt to attack the morale of the enemy and alter the perception of their organization by outsiders. Third, terrorists use the internet to build relationships with other groups so they can support one another in their actions. Fourth, terrorists use the internet to gather information and train members. This is made much easier through the use of videos posted online (Bocij, 2006).

The term "cyberterrorism" is also used to reference hacking campaigns with political or ideological motivations. One early case of cyberterrorism occurred in 2003 when Rajib Mitra hacked into a police emergency radio system. U.S. authorities labeled this an attack on the critical infrastructure of the country. Mitra was charged under the federal Computer Fraud and Abuse Act, convicted, and then sentenced to 96 months in prison. In 2004, David Jeansonne sent a malicious e-mail attachment to users of the MSN TV site so their computers dialed 911. He was charged with cyberterrorism under the USA PATRIOT ACT.

In October 2015, officials from the U.S. Justice Department charged a Malaysian, Ardit Ferizi, after he hacked into a server of an online retail company and stole personal data of U.S. service members (names, e-mails, passwords, and phone numbers). He then gave the information to members of the ISIS so they could carry out attacks on them. ISIS then threatened the victims with the following message: "We are in your e-mails and computer systems, watching and recording your every move, we have your names and addresses, we are in your e-mails and social media accounts, we are extracting confidential data and passing on your personal information to the soldiers of the [caliphate], who soon with the permission of Allah will strike at your necks in your own lands" (Davidson, 2016). He was charged with cyberterrorism, specifically, four counts of hacking into the company's server with the intent to assist the activities of the ISIS, extortion, and identity theft.

One hacking group that has attempted to identify and attack terrorist organizations is the Ghost Security Group (GSG), also called Ghost Sec. This is a vigilante computer hacking group that was originally created to not only target ISIS websites but also target the online activities of all extremist groups. The members describe themselves as a counterterrorism organization that uses the internet to "attack" terrorism. Their goal is to stop acts of terrorism and save innocent lives. They may be an offshoot of the hacking group Anonymous.

The members allegedly became more active after the shooting at Charlie Hebdo in 2015. The members monitor and collect data on the activities of terrorist groups and reports those activities, along with any threats, to law enforcement around the globe. The group claims that they have shut down hundreds of ISIS-affiliated websites and thousands of social media accounts in over a dozen different countries, including the United States, Germany, Italy, and Britain. They also have been able to infiltrate jihadi networks and provide enough information to law enforcement to prevent possible terrorist attacks. They have attacked sites used by ISIS to recruit new members. Some have reported that the GSG helped in stopping a planned terrorist plot in Tunisia and a plot to attack New York City in 2015. The members allegedly continue to scan the internet for newly emerging groups.

Chances are that events labeled as cyberterrorism will continue to rise as more governments, militaries, and civilians rely on computers to store data or to communicate. The opportunities for cyberattacks increases each day. At the same time, some people claim the fear of cyberterrorism held by the government and the public is exaggerated, largely because of movies that depict hackers who start a nuclear war or disable infrastructure. However, the majority of critical infrastructure is privately owned and not connected to the internet. While outsiders can hack these systems, it is difficult, and hacking into these systems does not provide offenders with the impact they seek (Gillespie, 2016). The effects of a cyberattack would be far less than what some people have described. Moreover, the majority of cyberterrorists are not able to carry out a major attack and cause a substantial impact because they do not have the technical skills that are needed to carry out such an attack. Instead, they would be forced to hire someone outside of their organization who would be willing to carry out the crime. To date, no one has died from a cyberattack. The actual risk of an attack on the country's critical infrastructure is far less than what has been described.

See also: Anonymous; Computer Fraud and Abuse Act of 1986; Operation Olympic Games

Further Reading

Akhgar, Babak, Andrew Staniforth, and Francesca Bosco. 2014. *Cyber crime and cyber terrorism investigator's handbook*. Waltham, MA: Elsevier.

Berinato, S. 2002. "The truth about cyberterrorism." *CIO Magazine*, March 15, 2002. http://www.cio.com/archive/031502/truth.html.

Bocij, Paul. 2006. *The dark side of the internet: Protecting yourself and your family from online criminals*. Westport, CT: Praeger.

Brenner, S. W. 2008. *Cyberthreats: The emerging fault lines of the nation state.* New York: Oxford University Press.

Charlton, Corey. 2017, February 15. "Keyboard warriors: Inside the "Ghost Security Group" hackers waging war on ISIS who claim to have foiled terror plots in Britain and over a dozen countries." *The Sun*, February 15, 2017. https://www.thesun.co.uk/news/2869317/ghost-security-hackers-isis-foiled-terror-plots-britain/

Council of Europe. 2007. *Cyberterrorism: The use of the internet for terrorist purposes*. Strasbourg Cedex, France: Council of Europe Publishing.

Davidson, Joe. 2016. "ISIS threatens feds, military after theft of personal data." *The Washington Post*, January 31, 2016. https://www.washingtonpost.com/news/federal-eye/wp/2016/01/31/isis-threatens-feds-military-after-theft-of-personal-data/?utm_term=.0136baeb6e55

Denning, Dorothy E. 2000. "CYBERTERRORISM: Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives." May 23, 2000. http://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm

Ghost Security Group Website. https://ghostsecuritygroup.com/

Gillespie, Alisdair A. 2016. *Cybercrime: Key issues and debates*. New York: Routledge.

Holt, Thomas J., George W. Burruss, and Adam M. Bossler. 2015. *Policing cybercrime and cyberterror*. Durham, NC: Carolina Academic Press.

Paganini, Pierluigi. 2016. "The Ferizi case: The first man charged with cyber terrorism." Infosec Institute, March 9, 2016. http://resources.infosecinstitute.com/the-ferizi-case-the-first-man-charged-with-cyber-terrorism/

Singer, Peter W. 2012. "The cyber terror bogeyman." Brookings, November 1, 2012. https://www.brookings.edu/articles/the-cyber-terror-bogeym

CYBERWARFARE

Cyberwarfare is a term that is not really well defined. The U.S. Department of Defense defines it as "the art and science of fighting; of defeating an opponent without spilling their blood" (Carr, 2010, p. 2). Experts at the Rand Corporation present a different definition. They say that cyberwarfare "involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks" (Rand, n.d.). Each cyberattack can be very different, depending on the skill of the hackers or their ultimate goal. An attack may be very harmful or relatively less so. The severity of an attack will differ and depend on the number of people that were affected and the damage caused. The immediacy of the attack (how long it lasted, or its duration) will also help to determine the severity as will the directness (the harm caused).

Cyberwarfare can be thought of as "virtual conflict" that involves the use and targeting of computers and the networks for war—or attacking another nation through the internet. It can be thought of as a politically motivated attack on another's computer systems, used to disable critical infrastructure systems (power, water, electricity), disrupt government, or steal data. It occurs when different nations, international organizations, or terrorist organizations break into the computers or networks in another country in order to cause damage, or to steal defense secrets or industrial technology. They can also go after information on business secrets like possible mergers or acquisitions. Those with more information are at an advantage. This warfare usually involves states—it is not usually done by individuals or groups.

Government websites have been prime targets for cyberwarfare. In 2008, Russia carried out a cyberattack on the website of the Georgian government. On July 4 weekend and the week after, in 2009, a DDoS attack was carried out on websites of the U.S. government, namely, the Federal Trade Commission (FTC) and Department of Treasury as well as commercial sites in the United States and South Korea. The attack took down the sites for several days. Eventually, the South Korean government blamed the Democratic People's Republic of Korea, but officials in the United States did not announce any formal opinion on the incident. Then in April 2009, a cyberattack compromised the security surrounding the Joint Strike Fighter project from the Pentagon, and several terabytes of data were stolen. Officials believed the hackers were from the People's Republic of China.

Then in December 2015, a cyberattack on the power grid for Ukraine affected 80,000 people who were without power for six hours. The governments of Georgia and Russia had been in a conflict after Russia seized the Crimea. Throughout the conflict, both countries used cyberwarfare.

Cyberwarfare does not require a strong military or a lot of money to launch an attack. Instead, it can be carried out by any country that has the right tools. This can be done through viruses or DoS attacks that shut down computers and networks. It can also be done by sabotaging systems to disrupt military and banking systems. So in a way, it allows a poor nation to be on a more equal footing as a more wealthy country. It used to be that stronger nations had more power, and they were strongest in world politics largely because of their military strength. But with the advent of cyberwarfare, small countries and nation-states can garner attention and affect politics when they were unable to in the past. The small nations that once lacked power have become serious threats to the powerful nation-states. They are able to collect information about military actions; can launch cyberattacks that will cripple computers; can block communications; all they need is access to a computer and the skill to hack into these systems.

Even though cyberwarfare is carried out online, it still can be a great threat to international peace and security, so countries seek to deter or prevent such attacks. The ability of a government to prevent an attack is not easy, but at the same time, the need to protect data belonging to the government, businesses, and individuals is critical. Methods must be updated and developed to protect against attacks. Even in those cases where law enforcement or the military identifies an attacker, the government of that country may not do anything about it. There is no international law that prescribes the rules for cyberwar: there are rules for war but not for cyberwarfare.

After an attack occurs, it is sometimes difficult to determine who or what country was responsible. There is often a lack of proof as to who did it. The offender will rarely admit to carrying out the attack, but the government, agency or business that is the victim may not want to publicize that they were the victim of an attack. They may not want to show their weakness or vulnerability to others or to customers. They also may not want to cause fear in its citizens. Thus, many attackers get away with these crimes.

See also: Distributed Denial-of-Service Attack (DDoS); Operation Olympic Games; Syrian Electronic Army

Further Reading

Carr, Jeffrey. 2010. *Inside cyberwarfare*. Sebastopol, CA: O'Reilly Media.

Gillespie, Alisdair A. 2016. *Cybercrime: Key issues and debates*. New York: Routledge.

RAND Corporation. n.d. "Cyberwarfare." http://www.rand.org/topics/cyber-warfare.html

Schmitt, M. N. 2011. Cyber operations and the *jus ad bellum* revisited. *Villanova Law Review* 56: 596–606.

Schmitt, M. N. 2013. *Tallinn manual on the international law applicable to cyber warfare*. Cambridge, UK: Cambridge University Press.

D

DARK WEB

When most people use the internet, they are using the surface web, which includes any sites that can be located through using a typical search engine such as Google, Bing, or Yahoo. There are many sites that are invisible or hidden to the majority of users, and these make up the deep web, also called the hidden or invisible web. The sites on this are not indexed by the usual search engines and will not appear on a typical computer search. The dark web is a smaller fraction of the deep web. The dark web is the portion of the internet that is an active marketplace for illegal items, such as weapons, drugs (black tar heroin, cocaine, and synthetic drugs), banned books, stolen credit card numbers, malware and hacking tools, and pornography. For example, information from the stolen credit cards, accessed during the Target data breach in December 2013, was sold on the dark web for a price that ranged from $20–135 (Ablon et al., 2014).

One popular and well-known dark web site is Silk Road 3, which openly sells illegal drugs and weapons. This is a newer version of the same site that has been shut down numerous times. The original Silk Road site was one of the first dark web sites that sold illegal products including computer equipment, drugs and drug paraphernalia, pornography, fake identification cards, and stolen credit card information, among other illegal items. The site was named after land trade routes that were used to transport goods from India, Asia, and Europe. In October 2014, agents from the Federal Bureau of Investigation (FBI) seized the site's server and arrested the owner, Ross William Ulbricht, also known as Dread Pirate Roberts. He was in San Francisco at the time the site was taken down. The courts charged him with drug trafficking, soliciting murder, enabling computer hacking, and money laundering. Law enforcement also seized millions of dollars in Bitcoins. Roberts was found guilty and sent to prison for life.

There are many other popular sites on the dark web. Darknet Heroes League (DHL) is one of those sites. They offer drugs, including stimulants, cannabis, opioids, and steroids, among others. A site called Mollyworld makes MDMA (3, 4-Methylenedioxymethamphetamine, commonly known as ecstasy) products available for sale. This site is one of the top suppliers of MDMA. The Dark Market offered stolen IDs and credit cards for sale. The site was shut down in 2008 after being infiltrated by the FBI. During the investigation, over 60 people were arrested around the world. Carder was a site that sold credit cards and other stolen financial information to interested buyers. The site was taken down in March 2012. Another popular site on the dark web is a hidden wiki that contains instructions for illegal activities such as making bombs.

It is not illegal to get on the dark web, but the items for sale are generally banned. The goods that are available for sale are constantly changing to reflect the needs of the consumer and new developments in technology. There is no money exchanged for the items bought and sold. Instead, transactions are carried out using cryptocurrency, like Bitcoin. The transactions are quick and efficient and usually untraceable.

The Dark Web can be accessed by people all around the world. Users do not need to have any special training or skills to access the dark web. The buyers can be individuals, criminal groups or vendors. They all have different skill levels. It has been estimated that approximately 80 percent of users on the dark web were free-lance (individuals), whereas the remainder of users were members of criminal organizations or groups (Ablon et al., 2014). A person must use specialized encryption software and browser protocols to access the dark web. A user must download software that allows them to open a portal. Many people use the Onion Router (Tor), which was developed by officials at the U.S. Naval Research Laboratory in response to a need for private communication. It is a free encryption protocol that hides the IP addresses and location of the user so the searches are private. If a user relies on a Tor, someone could tell they used it, but their ISP is not available.

Another way to ensure privacy while using the dark web is to use a virtual private network (VPN) that encrypts the internet activity of the user, thus permitting the user to search sites without revealing their identity. The VPN will also allow someone to rely on a shared IP address with other users. This also can prevent law enforcement from identifying a user's physical location.

It is fairly easy to get onto the dark web. After a person downloads the Tor browser, they can then register with a Darknet market by creating a username and password. The user can then purchase Bitcoins and send them to the Darknet Market Wallet. After searching the dark web and deciding on an item, the Bitcoins will remain in an escrow until the purchase is complete. Some buyers pay prior to receiving the product, but there have been case where no product arrives, and the buyer loses that payment.

Activities on the dark web are regularly monitored by law enforcement officials. They track who is visiting particular sites and how often they go there. Because the searches are private, and because purchases can be made anonymously, law enforcement sometimes struggles with confronting users on the dark web. However, law enforcement is becoming more effective in tracking what is sold and to whom.

Some parts of the dark web are harder to access than others, and in some cases the buyer must be vetted before they are allowed to access the site. These sites are frequently protected and require users to log in with a password in order to access it. Users must have established a good reputation among the hacking community in order to have access. They must be trusted by others, and they must know that the user has the skills to use the products.

The number of people who access the dark web and make purchases on it will probably increase simply because it is easy to access and it is becoming more widely publicized. There are also more sites available that sell banned goods that people have a desire to buy. Moreover, sellers make a large profit from selling banned items. Selling products on the dark web can be more profitable than the illegal drug trade (Ablon et al., 2014). Sellers can market their products to people around the world. In some cases, no physical product is needed. The buyer is able to download the item in just a few seconds without any interaction between the buyer and seller.

See also: Bitcoin; Cryptocurrency; Federal Bureau of Investigation; Malware

Further Reading

Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay. 2014. *Markets for cybercrime tools and stolen data*. Washington, D.C.: Rand Corporation.

Barratt, M. J., J. A. Ferris, and A. R. Winstock. 2014. Use of the Silk Road, the online drug marketplace, in the United Kingdom, Australia, and the United States. *Addiction*, 109: 774–783.

Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. 2018. *Cybercrime and digital forensics*. New York: Routledge.

Viswanatha, Aruna, and Robert McMillan. 2017. "Global crackdown shuts two of the dark web's biggest sites for drugs and guns." *Wall Street Journal*, July 20, 2017. https://www.wsj.com/articles/authorities-close-two-large-illegal-goods-websites-1500568971

DATA LEAKAGE

A data leak, or data spill, occurs when data or information is released without authorization and in an uncontrolled fashion. Personal details about an individual may be released, including social security numbers, personal credit and other financial information, or medical records. For companies, data leakage could lead to the distribution of confidential or propriety information, intellectual property, or private customer information.

The release of information can be intentional, but more often, data leakage is unintentional or inadvertent. This can occur in many ways. A file containing private data may be inadvertently or mistakenly sent to the wrong person (or multiple people) in an e-mail. Data leakage often results after an illegal hacking on the computer systems of a company that results in malware being uploaded, allowing a cybercriminal to access files. Some companies have become victims of phishing attacks, where e-mails sent to employees seem to be from the company (or elsewhere), but when the e-mails are opened, malware is introduced into the computer system. In some cases, a company falls prey to social engineering attacks. This happens when an employee receives a call from what appears to be another employee of the agency, typically a person at a computer help desk or IT, who explains that there is a problem with the computers. That individual then requests the password information or other sensitive information as a way to reset the system (or some similar scenario). In the end, the employee is duped into providing their password to the bogus employee, who then uses it to access files.

Data leakage is frequently the result of a disgruntled employee who releases information. In some situations, an employee has been offered money to provide confidential information to an outsider. This may happen if the business has a weak security system and an employee is able to access files beyond their authorization, or for a longer time than is needed. Employees have taken hard copies of files from an office setting or have taken pictures and removed information. In some cases, employees have been able to download information onto an external storage disk (a thumb drive or zip drive) and remove it from an office. There have also been cases where an office laptop computer with data has been stolen, or external storage drives have been lost or stolen.

There are many examples of data leakage. One of those is the breach of data from the retail giant, Target that occurred in December 2013. Hackers were able to access the names, mailing addresses, phone numbers, e-mails, and credit card information for 40 million Target customers, which is thought to have been sold on the black market. Target profits dropped almost 50 percent in the period immediately after the attack. Another example is the events surrounding Chelsea Manning, who stole thousands of classified and unclassified documents from military databases, and released them to WikiLeaks, which made them available online. While the data leakage from Target was the result of hacking, the data leakage by Manning was the result of a whistleblower.

Data leakage can be very damaging to individuals and organizations. For individuals, their private information is made public, leading to financial loss or loss of privacy. In a business setting, data leakage can result in lost productivity as employees need to spend time to discover how the information was accessed, then fix the leak or the problem. A data leakage can harm the reputation of a business, sometimes making customers unwilling to continue to frequent the business.

It is essential that organizations and businesses strive to prevent data leakage. To do this, companies need to upload antivirus products that prevent the installation of malware or detect malware if it is uploaded. Companies need to train their employees to recognize fake e-mails that could contain malware. All employees should be required to create and use secure passwords that are complicated, and they should then be prohibited from giving that password to anyone. Agencies should use encrypted platforms if sharing data to ensure that if a file is accessed by an unauthorized user, he or she will be unable to understand the data. Companies should upload software that scans outgoing e-mails and other messages to uncover the presence of data so that it is not released by mistake.

See also: Hacker and Hacking; Malware; Social Engineering; Sony Pictures Entertainment Hack

Further Reading

Dezenhall, Eric. 2015. "A look back at the Target breach." *Huffington Post*, April 6, 2015. https://www.huffingtonpost.com/eric-dezenhall/a-look-back-at-the-target_b_7000816.html

Huth, Carly L., David W. Chadwick, William R. Claycomb, and Ilsun You. 2013. "Guest editorial: A brief overview of data leakage and insider threats." *Information*

Systems Frontiers 15, 1: 1–4. https://link.springer.com/article/10.1007%2Fs10796-013-9419-8

Shabtai, Asaf, Yuval Elovici, and Lior Rokach. 2012. *A survey of data leakage detection and prevention solutions*. New York: Springer.

Van, Jon. 2008. "Firm's software helps stop data leaks." *Chicago Tribune*, May 26, 2008. http://articles.chicagotribune.com/2008-05-26/business/0805240033_1_data-leakage-encrypted-data-in-short-bursts

DATA SOVEREIGNTY

Data sovereignty refers to the idea that any data that has been stored in a binary digital format is subject to the laws and regulations of the country where that data is stored. In short, the computer data is controlled by the country in which it is located. This means that data that is located in one country cannot be subpoenaed by the government of another country. Some countries have gone so far as to pass laws that require that data and information remain in that country, largely a result of cloud computing and storage methods that make data easily transferrable. Governments are nervous about the ability of other countries or individuals to access their information or the information of their citizens.

Data sovereignty also refers to an individual person's right to control access to, and any disclosure of, their own personal information. This is violated when another person or when a government accesses that data. At that point, it becomes an issue of the power of the government to use their power of surveillance for security versus a person's rights to privacy.

The concept of data sovereignty became more widely debated in 2013 after a U.S. federal magistrate ordered that Microsoft provide the Department of Justice with information regarding a drug-related criminal case. The records were held in Dublin, Ireland. Officials at Microsoft would not provide the information, relying on laws from the European Union intended to protect the privacy of individuals. The case went to the court system, and the lower courts decided that companies within the United States must give private information to the government if there is a valid search warrant. Microsoft appealed that decision, and the Second Circuit appeals court sided with Microsoft in *Microsoft v. United States*, declaring that Microsoft was not required to provide information to the Department of Justice. They declared that search warrants issued in the United States do not apply to customer data that is stored abroad. The government appealed, and the case was heard by U.S. Supreme Court (this time as *United States v. Microsoft*), but was rendered moot in 2018 by legislation passed by Congress in the CLOUD Act, or Clarifying Lawful Overseas Use of Data.

Data sovereignty became a major issue again in 2013 when Edward Snowden, an employee at the National Security Agency, revealed classified documents describing extensive government surveillance programs on private individuals. Many people around the world began to question the rights of governments to collect personal data on citizens, particularly if there is no security threat posed. The law goes into effect on January 1, 2020.

There are currently no laws in the United States to protect the privacy of consumer data. Some states have passed laws, such as the California Consumer Privacy Act passed in 2018. This was a bill that gave citizens the right to tell a business not to share their personal information with other businesses; to limit what information is collected about yourself; and makes businesses responsible for leaking that data.

In 2016, the Parliament of the European Union passed a new law called the General Data Protection Regulation (GDPR). The law is comprised of 11 chapters and 91 articles and is intended to protect the privacy of data owned by all EU citizens, regardless of the location of the data or the company. If the company provides goods or services to EU citizens, they are subject to the law.

The law gives individuals more control over their personal data. If a company wants to gather personal information on an individual who lives in the EU, they must first ask permission before collecting that information and receive that person's consent. Any data that is collected must be maintained in a way that makes the data anonymous. If the data is breached, a customer must be informed of that breach within 72 hours of discovery. They must be provided with details of the breach. All companies must have a data protection officer to ensure compliance with the regulations. Companies must institute data protection measures to help protect against a breach. Any individual may ask a company to delete their personal information at any time.

The law assigned high fines on violations of the law. Any company that violates the law can be fined up to 4 percent of the profit, or 20 million Euro.

See also: Cybersecurity

Further Reading

EU GDPR. Eugdpr.org.

Farivar, Cyrus, and David Ingram. 2019. "California's new data privacy law could change the internet in the U.S." NBC News/CNBC, May 14, 2019. https://www.cnbc.com/2019/05/14/california-consumer-privacy-act-could-change-the-internet-in-the-us.html

Hardy, Quentin. 2014. "Cisco: The internet needs more control." *The New York Times*, September 29, 2019. https://bits.blogs.nytimes.com/2014/09/29/cisco-the-internet-needs-more-control/?mtrref=www.google.com&gwh=FE5B04EC0365E71990D3E25169006499&gwt=pay&assetType=REGIWALL

Hutzik, Michael. 2019. "Big business is trying to gut California's landmark privacy law." *Los Angeles Times*, April 19, 2019. https://www.latimes.com/business/hiltzik/la-fi-hiltzik-cal-privacy-act-20190419-story.html

Starks, Tim, and Gautham Nagash. 2013. "America, spooked." *CQ Magazine*, June 17, 2013. https://library.cqpress.com/cqweekly/document.php?id=weeklyreport113-000004296384&type=hitlist&num=0

DECRYPTION, *see* ENCRYPTION

DEF CON

DEF CON is the largest hacking conference, which is held every year in Las Vegas, Nevada. Founded in 1993 by Jeff Moss (and others) as a party for a fellow hacker, the name either comes from the phone dial, which has the letters "DEF" on the number 3, or from the military "Defense Condition" term, DEF CON, a reference to the movie *WarGames* (1983). According to the organization's website, the organizers of the conference do not aim to teach attendees how to hack a computer during the weekend-long conference; however, they seek to bring together people from various backgrounds who are all interested in cyber security. Many different types of people attend the conference, from computer security professionals to lawyers and hackers with an interest in the subject, both from the United States and internationally. Law enforcement officials attend the conference to see the new techniques and learn about trends. At DEF CON 2000, the Central Intelligence Agency (CIA), Department of Defense (DOD), and National Security Agency (NSA) held a panel called "Meet the Fed," where they attempted to recruit hackers to their agencies. The conference organizers held a contest to see who could "spot the fed." If an attendee was able to point out a federal employee, they won a T-shirt that said "I Spotted the Fed," and the agent received an "I Was the Fed" shirt (Furnell, 2002).

There are hands-on experiences for both guests and speakers. Throughout the conference, new hacking tools are presented, along with new skills and techniques for hacking. Attendees can test their hacking skills in a yearly "capture the flag" event in which participants must hack into specially designated machines and try to compromise as many machines as possible. It is a contest where teams of hackers test their skills by either attacking or defending networks. Dell and Symantec provide equipment. There are multiple speakers on a variety of subjects pertaining to cybercrime and security. Some of the topics presented at DEF CON 8.0 included "Evading Network-based Intrusion Detection Systems," "Advanced Buffer Overflow Techniques," "Penetrating B1 Trusted Operating Systems," and "Federal Computer Fraud and Abuse Act."

A component of DEF CON is Biohacking Village. Biohacking refers to the process of exploiting genetic material for personal or possibly for criminal reasons, and it often involves "backroom" experiments on a person's DNA that are not affiliated with a university or medical lab. The process of biohacking often involves individuals, called "grinders," who carry out experiments on themselves just to see what the results may be. For example, they may use implants or other technology to alter or improve their bodies or minds, a practice referred to as "do-it-yourself biology." Some grinders have attempted to carry out DNA or genetic testing at home. The Biohacking Village at DEF CON also provides information on biosecurity and personal information security, including methods to reduce risks of information loss. Conference attendees discuss the issues surrounding methods to protect massive databases comprised of personal medical information.

Packet Hacking Village is a popular component of DEF CON. This is a way to educate people about the need for better cybersecurity to protect people's personal information. The convention provides many methods to illustrate this need. One is the "Packet Detective" that shows users how to install network forensics tools, how to read others' e-mails, or how to detect usernames and passwords, and listen to phone conversations on the network. Each year the group has a Wall of Sheep that identifies bad security practices. They provide hands-on training that helps people understand how to secure end points such as laptops, desktops, and even phones. They also help people recognize advanced threats to their systems. They have sessions on how to improve security to prevent attacks or contain ones that may be running in a system.

In the Tamper-Evident Village, people learn how to recognize if a product's tamper-evident seal (adhesive seals, electronic tamper seals, evidence bags) has been damaged. Conversely, attendees are also taught how to erase any evidence that they have tampered with such seals. The program makes people understand how these products work and makes them aware that these protections are not always foolproof. Many tamper technologies are fairly simple and easy to destroy, but others are much more complex. This part of DEF CON shows participants how these technologies work and how they can be manipulated.

At each conference since 2011, the organization has held a Beard and Mustache contest to highlight the "intersection of facial hair and hacker culture." The three categories are full beard, partial beard or mustache only (for those with mutton chops, Van Dykes, or goatees), and freestyle.

See also: Hacker and Hacking

Further Reading

Def Con. https://defcon.org/

Furnell, Steven. 2002. *Cybercrime*. Boston, MA: Addison-Wesley.

Kevin2600. 2013. *DEFCON 20*. https://www.youtube.com/watch?v=rVwaIe6CiHw

Mak, Aaron. 2018. "The Most terrifying device hacks from this year's def con." *Slate*, August 13, 2018. https://slate.com/technology/2018/08/def-con-hackers-terrifying-technology-vulnerabilities.html

DENIAL-OF-SERVICE ATTACK (DoS)

A denial-of-service attack (DoS) occurs when a cybercriminal is able to disrupt services or connections to a website as a way to prevent users from having access to it. Criminals use a DoS attack to bombard a target site with requests that overload the system or network so the site owners are unable to respond to legitimate requests. Because a server can process a limited number of requests at one time, the mass flooding of requests will overload the server, shutting it down. Genuine users are unable to access information or services on the website. In some cases, a DoS attack will center on a victim's e-mail system. Most accounts have a limit on the number of e-mails or space that can be used, so an attacker will send hundreds of e-mails that will fill the space limit set by the system. This prevents the user from receiving legitimate e-mails. Attackers may prevent users from accessing their banking sites. Because users are unable to use the sites, their access to service has been denied (thus the name “denial-of-service attack”). In some cases, a DoS attack is used simply as a diversion, but others are serious attacks on computer systems.

A DoS attack originates from malware so that the company or owner may not be immediately aware of the attack. That means the attack can continue to attack the computer system for an extended time (weeks or even months) before it is recognized and stopped, making it very destructive. DoS attacks can harm a company’s productivity, as customers are unable to access their site, e-mail communication may be lost to customers, and down time results. The attacks may also result in a loss of profits to accompany, the theft of data and information, or even erosion of trust that the public has in that organization. Some attacks may even ruin network hardware, resulting in greater downtime and financial loss to repair equipment. If the attack is successful, a business may be required to spend thousands or even millions to not only fix damaged computer equipment but also prevent further harm to its professional reputation.

One variation on a DoS attack is an advanced persistent DoS attack. These are typically carried out by a person who has more advanced computer skills. In an Advanced Persistent DoS attack, multiple attacks are launched that sometimes last days or even weeks. They are very difficult to plan for or mitigate. Another variation is a Permanent DoS attack, also called phlashing. This kind of attack damages a network to such an extent that it must be replaced, sometimes a high financial burden to the company or organization. A more recent twist has seen cybercriminals demanding payment from victims in order to stop an attack from being launched, or to halt an attack that has been initiated. A third type of DoS attack is a permanent denial-of-service (PDoS) attack, which happens when a server is compromised to the point where it is not possible for the company or organization to regain control of it. Because of the seriousness of this type of attack, it is sometimes referred to as a “brick.” Other types of DoS attacks include buffer overflow, ping-of-death, SYN flooding, TCP, or teardrop.

In 2016, Twitter users were unable to access Twitter or faced slow periods and downtime. The disruption was caused by a DoS attack on the company. It was down for about two hours, and then was sporadic for a short time after that. Facebook also faced down time after a similar attack.

The DoS attack may have originated in a DEF CON conference held in Las Vegas where access to the internet was disrupted for one hour.

Many cybercriminals who launch a DoS attack are individuals or businesses, but these attacks can be launched by other governments. Some offenders seek to harm the organization or person under attack, ruin their reputation, or event cause damage to slow down their business. Some offenders use a DoS attack to steal data or information on the company or individuals. Some hactivists use a DoS attack as a way to shut down the website of an organization that they oppose or do not agree with.

According to the U.S. Computer Emergency Readiness Team (CERT), there are particular things to look for to identify if a company or organization has become the victim of a DoS attack. A company or organization may be experiencing slow network performance (such as difficulty opening web sites or files stored on the network), an inability to access the website (or access is slow), and an increase in the number of spam e-mails being received. Companies should look for changes in the traffic on their websites, looking for unexplained traffic or spikes.

It is important that companies and organizations create a plan to prepare for a possible DoS attack. If an attack begins, a company can reroute malicious traffic and limit the impact the attack has on their sites. There are products that are readily available to help companies and organizations that can be installed on networks to help them detect attacks quickly. Any kind of vulnerabilities should be identified and patched as a way to prevent an attack.

See also: DEF CON; Distributed Denial-of-Service Attack (DDoS); Malware

Further Reading

Nichols, Michelle and Louis Charbonneau. 2013. "Cyber attacks against the media on the rise, rights group says." Technology News, *Reuters*, February 14, 2013. https://www.reuters.com/article/net-us-media-cyberattacks-idUSBRE91D1LN20130214

Peterson, Andrea. 2016. "'Internet of Things' compounded Friday's hack of major websites." *Washington Post*, October 21, 2016. https://www.washingtonpost.com/news/the-switch/wp/2016/10/21/someone-attacked-a-major-part-of-the-internets-infrastructure/?utm_term=.e70d04d5e0b5

Van Buskirk, Eliot. 2009. "Facebook confirms denial-of-service attack." *Wired*, August 6, 2009. https://www.wired.com/2009/08/facebook-apparently-attacked-in-addition-to-twitter/

DEPARTMENT OF DEFENSE, ATTACKS ON

In 2007, an official working in the Pentagon opened a Twitter post appearing to be an offer for a family vacation. When the official clicked on the link, malware was quickly downloaded onto the official's computers, and they were instantly infected, giving Russian hackers access to the computer system at the Pentagon. It was discovered that the Russians had sent 10,000 Twitter posts to employees at the Department of Defense (DOD) that appeared to be from friends, a practice referred to as "Spear phishing." This occurs when hackers are able to send a malicious file through what appears to be a message from a friend or other safe source, and they are opened by unsuspecting employees.

The following year, in 2008, a USB flash drive was found in the parking lot of the DOD facility in the Middle East. The flash drive had been infected with malware that was uploaded onto every computer into which the zip drive was inserted. The malware was uploaded onto the network operated by U.S. Central Command. The malware spread quickly throughout the network and allowed cybercriminals in foreign countries to have access to both classified and unclassified information. The malware was undetected for weeks, giving foreign governments more or less unlimited access to key documents. After this event, officials at the DOD spent 14 months clearing their computers of the malware.

Officials from the DOD testified in front of Congress in 2009 and admitted that cyberattacks on the U.S. DOD had increased. Many of the attacks were said to have originated in China, but they were coming from many sources. The officials reported that in 2008, there were 54,640 malicious cyberattacks on DOD systems. Further, in the first half of 2009, there were 43,785 attacks. The United States paid somewhere around $100 million to protect the nation's computer systems against any future attacks.

The DOD suffered another hacking in March 2011. This time, the offending group was a foreign intelligence service that hacked into the computer system belonging to a corporate contractor who was developing a military system. The hacker was able to steal 24,000 files. Oddly enough, officials in the DOD had just released a new strategy to deal with cybercrime. The new strategy relies on a "dynamic defense" that entails looking for hackers before they attack. The DOD also sought to build more resiliency into the nation's computer system in case of an attack.

After this attack, the Pentagon officials in 2011 sought to impose a new policy whereby a computer attack carried out by a foreign nation could be considered to be an act of war that could result in some kind of a military response. The possible responses could include economic sanctions, retaliatory cyberattacks, or even military strikes. They argued that a cyberattack is a more modern form of a traditional act of war. Further, if the attack cut off power supplies or harmed hospitals, it could result in injuries or even casualties to citizens.

Despite the harsh rhetoric, the DOD continued to be the focus of attacks. In 2015, an unidentified British man was arrested for a cyberattack on the DOD. The hacking took place in June 2015, allowing for the theft of data from a messaging service that was used by DOD employees. The hackers stole personal details of approximately 800 people, including their names, e-mails, and phone numbers. However, the hackers stole no sensitive data and the attack did not compromise national security (Holden, 2015).

More recently, in 2015, an unclassified e-mail network used by Pentagon employees was attacked. Officials working in the DOD believed that Russia was to blame. Immediately after it was discovered, the Pentagon shut down the server for about 4,200 unclassified accounts, including the chairman of the Joint Chiefs of Staff, as a precaution. It seemed that the attack was persistent and evolved quickly. The DOD described the attack as a phishing attack.

The Russians are not the only group attempting to hack into the U.S. DOD. In 2016, for example, the Chinese government was accused of carrying out a cyberattack on a DOD contractor. In the past, it has been estimated that hackers from China were thought to have stolen millions of personnel records for the Office of Personnel Management, but officials in China have denied it.

See also: Cyberterrorism; Cyberwarfare; Hacker and Hacking; Social Engineering

Further Reading

Castle, Stephen. 2015. "U.K. arrest in cyberattack on American military." *International New York Times*, March 7, 2015. http://www.lexisnexis.com/lnacui2api/delivery/PrintWorking.do?

Holden, Michael. 2015. “Briton arrested over hack into U.S. Department of Defense.” *Reuters*, March 6, 2015. https://www.reuters.com/article/us-britain-usa-hacker-idUSKBN0M214K20150306

Lubold, G., and D. Paletta. 2015. “Pentagon sizing up email hack of its brass; Officials believe Russia was likely behind the cyberattack of the unclassified network.” *Wall Street Journal*, August 7, 2015. https://search.proquest.com/usmajordailies/pointviewfile?accountid=14471.

McMillan, Robert. 2009. “Security monitor report: China tied to cyberattacks on U.S. systems.” Computerworld, December 7, 2009. http://www.lexisnexis.com/lnacui2api/delivery/PrintWorking.do?delFmt=QDS

Nakashima, Ellen. 2010. “Defense official discloses cyberattack.” *Washington Post*, August 25, 2010. https://search.proquest.coom/usmajordailies/docview/755976410/fulltext/3E521BA9292940D5PQ/3?accountid=14471.

Paletta, Damian. 2015. “NSA Chief Syas cyberattack at Pentagon was sophisticated, persistent; Breach of Joint Staff’s unclassified network evolved from failed attack a week before.” *Wall Street Journal*, September 9, 2015. https://www.wsj.com/articles/nsa-chief-says-cyberattack-at-pentagon-was-sophisticated-persistent-1441761541

Sanger, D.E. 2011. “Pentagon to consider cyberattacks acts of war.” *New York Times*, June 1, 2011. http://wezproxy.uakron.edu:2048/login?

Shanker, Thom, and Elisabeth Bumiller. 2011. “After suffering damaging cyberattacks, the Pentagon takes defensive action.” *New York Times*, July 15, 2011. http://ezproxy.uakron.edu:2084/login?url=https://search.proquest.com/docview/876635079accountid=14471

DIGITAL CURRENCY

Digital currency is any currency that is digital in nature. In the United States and other places, consumers increasingly access money in a digital format, with a significant amount of banking being done online. Commercial transactions online, such as purchases on sites like Amazon or eBay, are completed digitally. Even in-person commercial transactions often take place in a digital format through the use of credit and debit cards. This digital currency is backed by physical currency at traditional financial institutions, such as banks and credit unions.

While traditional money is often represented in digital form and would fit the technical definition of a digital currency, the term “digital currency” is often used to refer to nontraditional currencies that are in digital form. One such form of digital currency that has emerged is cryptocurrency. Cryptocurrencies are completely digital in nature. They are not backed by physical currency like digital transactions of traditional currency are. Additionally, unlike transactions of traditional currency, cryptocurrencies have the added feature of decentralization—monetary transactions are verified not through a central organization like a bank, but through the use of a public ledger (blockchain) that is verified by numerous individuals (e.g., miners).

There have been digital currencies that fell somewhere between traditional currency in digital form and cryptocurrency. One such currency was e-gold, which was a digital currency backed by gold. E-gold was founded in 1996. At its peak, it operated in over 165 countries and processed over $1 billion in transactions annually (E-gold Blog, 2008). It was ultimately shut down by the Department of Justice. The owners of the company—Douglas L. Jackson, Reid A. Jackson, and Barry K. Downey—were charged with conspiracy to launder monetary instruments, operating an unlicensed money transmitting business, and money transmission without a license on April 24, 2007 (United States Department of Justice, 2007).

Traditional monetary transactions completed digitally are processed by traditional financial institutions, such as banks and credit unions. For transactions using cryptocurrencies and other non-traditional currency, a digital currency exchange would facilitate the transaction. Those exchanges allow customers to exchange digital currency (such as Bitcoin) for traditional currency (U.S. dollars, Euros, etc.). Several digital currency exchanges bring in millions in revenue a day (Russo, 2018).

Mt. Gox was a digital currency exchange that was, at one point, the world's largest Bitcoin exchange, handling 80 percent of all Bitcoin trading (Trautman, 2014). Before it was a Bitcoin exchange, Mt. Gox was a website dedicated to trading cards. Specifically, Mt. Gox handled the online trade of Magic: The Gathering cards. The name of the site is an acronym for Magic: The Gathering Online Exchange. The site kept the name after the company switched from card trading to Bitcoin exchanging. The site encountered financial troubles in 2014. On February 25 of that year, Mt. Gox shut the site down and declared bankruptcy. Those financial troubles stemmed from approximately 800,000 Bitcoin that went missing, with a value of over $400,000 at the time (Moore, 2014; Wieczner, 2018). It is believed that hackers stole some of those Bitcoin. Mt. Gox CEO Mark Karpelès ultimately discovered the location of 200,000 of the missing Bitcoin (Wieczner, 2018). As of late 2018, bankruptcy proceedings are still ongoing. It seems that Mt. Gox customers may ultimately receive some of their Bitcoin back (Wieczner, 2018).

An exchange may face regulation from the countries in which it operates. In some countries—such as Bolivia, Egypt, and the United Arab Emirates—digital currencies may be prohibited in general (Law Library of Congress, 2018). In other countries, the exchange of these currencies may be regulated. For example, in the United States, digital currencies may constitute securities for purposes of U.S. securities laws, and thus digital currency exchanges operating in the United States would have to register with the Securities and Exchange Commission (U.S. Securities and Exchange Commission, 2018).

Those involved with nontraditional digital currencies may face legal challenges. As noted above, the owners of e-gold were charged with various financial crimes. Mark Karpelès was arrested in Japan in 2015 for allegedly embezzling $3 million from the company (Ripley, 2019). In both these instances, there appears to be allegations that certain users of the services were to some degree criminally responsible for the disappearance of funds (see E-gold Blog, 2011; Ripley, 2019). Digital currency exchanges are not the only businesses that might face legal challenges. Businesses accepting digital currency may as well. An example of this is Silk Road—an online marketplace founded in 2011. The site was initially shut down in 2013 and its founder, Ross Ulbricht (who went by the name Dread Pirate

Roberts online), was charged and convicted for money laundering and drug trafficking (Segall, 2015). This case illustrates the concern law enforcement has with nontraditional digital currencies—the ability of them to be used to commit crimes without being tracked. Silk Road was notorious for being a place where drugs could be bought. In the press release announcing the indictment of the owners of e-gold, this concern was expressly mentioned. Said Assistant Director James E. Finch of the FBI's cyber division:

> The advent of new electronic currency systems increases the risk that criminals, and possibly terrorists, will exploit these systems to launder money and transfer funds globally to avoid law enforcement scrutiny and circumvent banking regulations and reporting. The FBI will continue to work closely with the Department of Justice and our federal and international law enforcement partners to aggressively investigate and prosecute any, and all, persons or organizations that use these systems to facilitate child pornography distribution, to support organized crime, and to perpetrate financial crimes. (United States Department of Justice, 2007)

The legal challenges faced are not limited to criminal charges. There could be civil repercussions as well. In the United States, lawsuits involving cryptocurrencies have risen exponentially in recent years. In the last quarter of 2017, there were seven securities cases involving cryptocurrencies. In the first two quarters, that number rose to 22 and 23, respectively (Lex Machina, 2018).

See also: Bitcoin; Cryptocurrency; Dread Pirate Roberts (Ulbricht, Ross; 1984–); Financial Crimes; Hacker and Hacking; Silk Road

Further Reading

E-Gold Blog. 2008. "E-Gold assists law enforcement, bringing hundreds of criminals to justice." E-gold Blog, March 11, 2008. https://blog.e-gold.com/2008/03/e-gold-assists.html.

E-Gold Blog. 2011. "E-Gold value access plan—Government forfeiture action." E-gold Blog, June 3, 2011. https://blog.e-gold.com/2011/06/vap-update.html

Hileman, Garrick, and Michel Rauchs. 2017. *Global cryptocurrency benchmarking study*. Cambridge, UK: Cambridge Centre for Alternative Finance.

Law Library of Congress. 2018. *Regulation of cryptocurrency around the world*. Washington, D.C.: The Law Library of Congress.

Lex Machina. 2018. "Lex Machina's 2018 securities litigation report reveals securities litigation is at an all-time high." *Lex Machina*, September 11, 2018. https://lexmachina.com/media/press/lex-machinas-2018-securities-litigation-report-reveals-securities-litigation-is-at-an-all-time-high/

Moore, Heidi. 2014. "The Mt Gox Bitcoin scandal is the best thing to happen to Bitcoin in years." *The Guardian*, February 26, 2014. https://www.theguardian.com/money/us-money-blog/2014/feb/25/bitcoin-mt-gox-scandal-reputation-crime

Ripley, Will. 2019. "The Carlos Ghosn case is putting Japan's system of 'hostage justice' under scrutiny." CNN, January 20, 2019. https://www.cnn.com/2019/01/20/business/carlos-ghosn-japan-justice-system/index.html

Russo, Camila. 2018. “Crypto exchanges are raking in billions of dollars.” *Bloomberg*, March 5, 2018. Retrieved from https://www.bloomberg.com/news/articles/2018-03-05/crypto-exchanges-raking-in-billions-emerge-as-kings-of-coins on October 5, 2018.

Segall, Laurie. 2015. “Silk Road’s Ross Ulbricht sentenced to life.” CNN, May 29, 2015. https://money.cnn.com/2015/05/29/technology/silk-road-ross-ulbricht-prison-sentence/index.html

Trautman, Lawrence. 2014. “Virtual currencies Bitcoin & What Now after liberty reserve, Silk Road, and Mt. Gox?” *Richmond Journal of Law & Technology* 20, 4, pp. 1–108.

United States Department of Justice. 2007. “Digital currency business E-Gold indicted for money laundering and illegal money transmitting.” United States Department of Justice, April 27, 2007. https://www.justice.gov/archive/opa/pr/2007/April/07_crm_301.html

U.S. Securities and Exchange Commission. 2018. “Statement on potentially unlawful online platforms for trading digital assets.” U.S. Securities and Exchange Commission, March 7, 2018. https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading

Wieczner, Jen. 2018. “$1 billion Bitcoins lost in Mt. Gox hack to be returned to victims.” *Fortune*, June 22, 2018. http://fortune.com/2018/06/22/bitcoin-price-mt-gox-trustee/

DIGITAL MILLENNIUM COPYRIGHT ACT

Congress passed the Digital Millennium Copyright Act (17 U.S. Code § 101 et seq.) on October 28, 1998. The Act addressed new and emerging issues related to copyright law and its transition into the age of the internet. It integrated two World Intellectual Property Organization (WIPO) treaties, as well as adding additional legislation. It does contain legislation on copyright matters that are not of a digital nature (there is a section that protects ship hull designs). However, the vast majority of the Act covers digital copyright issues.

One provision in the Act that was part of the incorporated treaties is the provision prohibiting the circumvention of digital rights management—technological means implemented by the author of a creative work to prevent illegal distribution of that work. The creation and distribution of devices that can circumvent digital rights management is also prohibited if those devices are primarily designed for circumvention. There are some exceptions to this rule. For example, nonprofit libraries and educational institutions can circumvent protective measures for the purpose of reviewing a work to determine whether they want to ultimately obtain the work. There is also an exception for encryption research—research designed to find vulnerabilities in protective measures for the purpose of fixing and improving those measures.

Among the legislation included in the Act outside the incorporated treaties is a provision that limits liability for ISPs. Specifically, the act limits the liability of these providers in instances where someone using their service engages in conduct that violates the copyrights of someone else. The service provider must not be involved in the conduct in order to be exempt from liability. Other legislation included outside the incorporated treaties includes an exemption to the general copyright laws for making copies of software when conduct computer repair, an exemption for nonprofit libraries and archives to transfer older works into a new format when that format becomes obsolete, and an exemption for broadcasters to make a copy of a work to assist in transmitting that work—such as recording numerous songs in a larger recording to broadcast instead of having to switch each song manually.

Technology has certainly advanced since 1998. Revision of U.S. copyright is something that is being contemplated. Three issues that directly deal with digital copyrights are mass digitalization, digital-first sales, and orphan works. Mass digitalization refers to process of making information available digitally in a large scale fashion. Libraries encounter this issue when deciding to what extent to digitize their books. Digital-first sales present an issue as well. In copyright law, a first sale is the initial transfer of a creative work to a purchaser. After that first sale has taken place, the purchaser is free to do what they wish with that purchase. For example, after buying a book from a bookstore, the consumer is free to do what they wish with that book from that point forward, such as sell it to a friend. With digital creative works, this often is not the case. Companies put restrictions on digital works and prohibit the purchaser from turning around and selling or lending that item. For example, after buying and downloading a video game from an online source, that game will often be tied to an account the purchaser creates. Because it is tied to an account, the company can (and does) prohibit transfer of the game to someone else, either for sale or just to let someone borrow it (Pallante, 2013). Orphan works are creative works where the author is unknown and unable to be determined. Orphan works can be physical in form, but they can also be digital. The legal treatment of orphan works impacts whether individuals and institutions may make use of such creative works, such as abandonware or orphaned writings that have been digitized. The U.S. copyright office has provided reports to Congress on all three of these issues (United States Copyright Office, 2001, 2006, 2011).

Maria Pallante, current register of copyrights for the United States, has stated she feels it is time for a revision of the copyright law (2013). Specifically, she has advocated a comprehensive revision, not piece-by-piece revisions. She believes the language of the copyright law should be simplified, namely because the number of people affected by copyright law is increasing. While she does point out numerous copyright issues that should be addressed in a comprehensive revision, she does not necessarily offer her opinion on those issues. Among the issues mentioned that have significance to digital works are those of incidental copies (copies of a creative work that exist often as part of an online purchase), digital first sale, and orphan works (creative works where the author is unknown and unable to be determined).

See also: Abandonware; Copyright Infringement; Digital Rights Management

Further Reading

Pallante, Maria A. 2013. "The next great Copyright Act." *The Columbia Journal of Law & the Arts* 36, 3: 315–344.

United States Copyright Office. 1998. *The Digital Millennium Copyright Act of 1998 U.S. Copyright Office summary*. Washington, D.C.: United States Copyright Office.

United States Copyright Office. 2001. *DMCA Section 104 Report*. United States Copyright Office. http://www.copyright.gov/reports/studies/dmca/dmca_study.html

United States Copyright Office. 2006. *Report on orphan works*. Washington, D.C.: United States Copyright Office.

United States Copyright Office. 2011. *Legal issues in mass digitization: A preliminary analysis and discussion document*. Washington, D.C.: United States Copyright Office.

DIGITAL RIGHTS MANAGEMENT

Digital rights management is a term that refers to the process of encoding digital intellectual property (e.g., music, videos, books, video games) in such a way as to prevent unauthorized distribution of that intellectual property. There are several ways this can be done. One method limits the number of devices to which a given item can be downloaded. This can be done by requiring online authentication with a server owned by the company that owns or distributes the intellectual property in question. Another method used is to code the file in question so that it can only be accessed via a company's approved media viewer. Although digital rights management has been used primarily to protect unauthorized distribution of intellectual property, it has been experimented with in other commercial arenas. Notably, Keurig—a coffee company—currently uses digital rights management to prohibit its coffee makers from brewing coffee from any unauthorized coffee pod. This is accomplished through the use of chips in the lids of authorized coffee pods that are then read by the Keurig coffee maker. Keurig appeared to be taking steps away from digital rights management in 2015, but it has not completely abandoned its use (Hern, 2015).

The stated need for digital rights management is that it helps prevent intellectual property theft. It is estimated that the annual cost to the U.S. economy from intellectual property theft could be as high as $600 billion (Commission on the Theft of American Intellectual Property, 2017). The circumvention of digital rights management is prohibited in the United States under the Digital Millennium Copyright Act of 1998, as is the creation of tools specifically designed to circumvent digital rights management.

There is some question as to whether digital rights management is advisable for companies to use. There is research that indicates that a company could see increased profits by not employing digital rights management (Zhang, 2014). Some companies have moved away from using digital rights management. As of January 6, 2009, Apple removed digital rights management from its song library on iTunes, with the participation of the four major music labels—Sony BMG, Warner Music Group, EMI, and Universal Music Group (Apple, 2009). Amazon's digital music library is also offered without digital rights management (Amazon, 2019). While the music industry appears to have generally moved away from digital rights management, other digital works—video games, movies, e-books—still regularly employ it. Some in those industries have advocated a move away from the use of digital rights management in their fields as well. Tommy Refenes, developer of the video game Super Meat Boy, has stated that the use of digital rights management can alienate dedicated customers, thus decreasing long-term sales (Thier, 2013). Charlie Stross, author of numerous science-fiction novels, expressed similar sentiments, noting that e-book publishers who removed digital rights management from their e-books were likely to benefit from the goodwill this would generate among their customers (2012).

The arguments against digital rights management extend beyond whether or not it is truly more profitable in the long run to employ it. There is argument that the use of digital rights management can hinder people who have purchased digital creative works from performing acts which are legal under the copyright law. For instance, U.S. copyright law does permit use of copyrighted works without permission of the copyright holder in some limited instances under the fair use doctrine. Additionally, U.S. copyright law permits the owner of a computer program to create an archival copy (i.e., backup copy) of that program (USC, Title 17 § 117). Digital rights management can make such a process difficult if not impossible. Some companies add an end user agreement to its computer programs indicating the creation of an archival copy is in violation of that agreement. While this might render the argument over archival copies moot, as mentioned above, there is concern that practices like this may alienate customers and do more harm than good in the long run.

Another argument against digital rights management are concerns that companies using digital rights management may overreach in their attempts to prevent copying of their creative works. Indeed, Sony BMG was involved in such an incident. On October 31, 2005, Mark Russinovich—a computer programmer—discovered that as part of their digital rights management, Sony BMG was downloading what amounted to a root kit—a program that allows unauthorized access to a computer without the owner of that computer being able to detect the intrusion—on the computers of customers using its CDs. No mention of the software or the fact that it would be installed on the computer of users was mention in Sony BMG's end user agreement (Russinovich, 2005). The hidden nature of the software coupled with its ability to allow unauthorized access to computers it was downloaded on rendered those computers vulnerable to exploitation by those looking to disseminate computer viruses. This is ultimately what happened (BBC News, 2005). Compounding the problem was the fact that, once installed, the software was difficult to remove from computers. This eventually led to a number of lawsuits being filed against Sony BGM in the United States. It settled several of these cases, costing it over $5 million (McMillan, 2006). It also faced a federal class action lawsuit in the United States (Associated Press, 2005).

There have been efforts made by several organizations to push back against the use of digital rights management. There is an International Day against DRM (digital rights management) that is sponsored by the organization Defective by Design. It was first celebrated on October 3, 2006. The organization Creative Commons offers various licenses, free of charge, that people can use to license their creative works without digital rights management and without other copyright encumbrances.

See also: Copyright Infringement; Digital Millennium Copyright Act; Rootkit

Further Reading

Amazon. 2019. “About media formats.” https://www.amazon.com/gp/help/customer/display.html?nodeId=201379550

Apple. 2009. “Changes coming to the iTunes store.” Apple, January 6, 2009. https://www.apple.com/newsroom/2009/01/06Changes-Coming-to-the-iTunes-Store/

Associated Press. 2005. “Sony BMG tentatively settles suits on spyware.” *New York Times*, December 30, 2005. https://www.nytimes.com/2005/12/30/technology/sony-bmg-tentatively-settles-suits-on-spyware.html

BBC News. 2005. “Viruses use Sony anti-piracy CDs.” *BBC News*, November 11, 2005. http://news.bbc.co.uk/2/hi/technology/4427606.stm

Commission on the Theft of American Intellectual Property. 2017. *Update to the IP Commission report*. Seattle, WA: The National Bureau of Asian Research.

Hern, Alex. 2015. “Keurig takes steps towards abandoning coffee-pod DRM.” *The Guardian*, May 11, 2015. https://www.theguardian.com/technology/2015/may/11/keurig-takes-steps-towards-abandoning-coffee-pod-drm

McMillan, Robert. 2006. “Sony rootkit settlement reaches $5.75M.” *PCWorld*, December 22, 2006. https://www.pcworld.com/article/128310/article.html

Russinovich, Mark. 2005. “Sony, rootkits and digital rights management gone too far.” Microsoft TechNet (blog), October 31, 2005. https://blogs.technet.microsoft.com/markrussinovich/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far/

Stross, Charlie. 2012. “The case against DRM on eBooks.” *Gizmodo*, April 25, 2012. https://gizmodo.com/the-case-against-drm-on-ebooks-5905023

Thier, Dave. 2013. “DRM Hurts Companies More than Piracy, Developer Argues.” *Forbes*, March 19, 2013. https://www.forbes.com/sites/davidthier/2013/03/19/drm-hurts-companies-more-than-piracy-developer-argues/#372de7716aa6

United States Copyright Office. 1998. *The Digital Millennium Copyright Act of 1998 U.S. Copyright Office Summary*. Washington, D.C.: United States Copyright Office.

Zhang, Laurina. 2014. “Intellectual property strategy and the long tail: Evidence from the recorded music industry.” *Researchgate*. https://www.researchgate.net/publication/275639877_Intellectual_Property_Strategy_and_the_Long_Tail_Evidence_from_the_Recorded_Music_Industry

DIGITAL SIGNATURES

Most companies today rely on electronic documents and signatures as part of their basic business operations. Documents must be signed by people in different offices who may be located in a different state or even in a different country. But it is sometimes difficult to know if a signature is valid or the document is original. A digital signature is a method for determining the authenticity of digital documents. A digital signature is the equivalent of a handwritten signature in the digital environment. These are important when documents are sent via e-mail. With a digital signature, the document is authenticated as the original document, and it verifies that the document has not been modified in any way. They are often used when a contract is sent to another location, to ensure the accuracy of financial transactions, or to verify the legitimacy of other business documents. A document with a digital signature, such as a birth certificate, a driver’s license, bank statement, or passport, will be unlikely to be forged or altered. Legally, digital signatures are accepted the same as handwritten signatures and imply consent by the signer. In short, digital signatures ensure both the authentication and integrity of the digital record because it makes it impossible to forge or alter the document without others knowing.

A digital signature is a type of electronic signature that involves the use of a mathematical algorithm that generates two long numbers, referred to as keys. The public key infrastructure, or PKI, helps to create the two keys. One of the numbers (keys) is public, and the other remains private. When a person signs electronically, the signature uses the private key. The algorithm encrypts the data, called hash, which becomes the digital signature. When the recipient receives the hash (the encrypted document), they also receive the public key, which is used to decrypt the document. If the decrypted hash matches the second, public key, it indicates that the data has not been tampered with since it was signed by the sender. If the data is altered, the document cannot be decoded, and the digital signature is no longer valid. Many different companies have developed software that provides the technology for people who wish to use digital signature to send documents electronically.

If a person uses a digital signature on a document, it makes it very difficult for them to deny that they sent it. It also verifies that the recipient received it in the original format that was sent to them. Since they are also time-stamped, the date and time of signing is also documented.

Even with the process of digital signatures, there is still concern about the safety and legitimacy of the process. In 2000, the U.S. Congress passed the Electronic Signatures in Global and National Commerce Act, otherwise known as ESIGN (Public Law 106–229, 15 U.S.C. 96). This new law was an attempt to simplify and encourage the use of electronic or digital signatures in interstate and international commerce. The law mandated that an electronic signature is legal. It prohibits a person from denying the legality of a contract or transaction on the basis that the signature or document is in electronic form. In essence, the law made electronic signatures the equivalent to a personal signature. Digital signatures were the focus of additional federal attention in 2010 when Congress worked with the leaders of major companies to pass a resolution to recognizing June 30 as "National ESIGN Day."

In 1998, President Bill Clinton recognized the importance of digital signatures in foreign commerce. In a joint statement about electronic commerce with Japan, he noted that it was important for governments to support the development of a global framework to recognize and facilitate electronic transactions. He suggested that countries develop a legal framework for developing regulations on digital signatures. In doing so, he proposed including members of the private sector in constructing the rules, that electronic signatures be legally recognized as the equivalent to handwritten ones, and that those involved in a transaction be allowed to determine the most appropriate method to authenticate the documents and signatures (Clinton, 1998).

See also: Encryption

Further Reading

Alexander, Karen. 2000. "E-Signature law opens new doors for security firms." *Los Angeles Times*, July 1, 2000. https://www.latimes.com/archives/la-xpm-2000-jul-01-fi-46644-story.html

Blanchette, Jean Francois. 2012. *Burdens of proof: Cryptographic culture and evidence law in the age of electronic documents*. Cambridge, MA: MIT Press.

Clinton, William J. 1998. "United States-Japan Joint Statement on Electronic Commerce." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, May 15, 1998. https://www.presidency.ucsb.edu/documents/united-states-japan-joint-statement-electronic-commerce

U.S. Department of Commerce, Information Technology Laboratory, National Institute of Standards and Technology 2013. *Digital signature standard (DSS)*. Gaithersburg, MD. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.186-4.pdf

DISTRIBUTED DENIAL-OF-SERVICE ATTACK (DDoS)

A DDoS attack occurs when an attacker gains control over others' computers, called zombies, and uses those computers to send repeated messages to a particular website so that the website is not able to keep up, most often causing the site to crash. The U.S. Computer Emergency Readiness Team (CERT) defines a DDoS attack as being characterized by an attempt by attackers to prevent legitimate users of a service from using that service. For businesses, it could mean a significant loss of revenue.

Different types of DDoS attacks have been used in the past. One is an attack that is geared toward overloading a target. Another kind of attack targets flaws in a network and then overwhelms the targeted system. A third type of attack is one in which the networks or databases are deluged with a high volume of calls, sometimes hundreds or even thousands of calls per hour. In the end, all types of attacks have the end goal of taking a site offline for a period of time.

One common method of carrying out a DDoS attack is for an attack to send an e-mail to an employee at a company that appears to be from a legitimate or known sender, asking the employee to look at a file. However, unbeknown to the recipient, the e-mail attachment contains malware that automatically uploads a program, allowing the cybercriminal to control the recipient's computer. The cybercriminal then is able to access all of the files that the recipient can access. When an offender is able to collect passwords and information in this way, it is called "social engineering."

In some cases, the cybercriminal will have a program to find a susceptible computer system (one with some kind of vulnerability or weakness, or one that does not have security patches maintained) and download a program that will make the newly infected computer a DDoS master. This means that the assailant will be able to use this system to identify other susceptible computer systems, upload malware onto them, and gain control over them as well.

When a cybercriminal gains control over many computers, whether through social engineering or any other method, the assailant is referred to as a "botmaster," and the computers that the cybercriminal controls are called “zombies,” or “botnets.” The assailant will then use the zombie computers to spread the malware to even more systems through e-mails. Once the attacker controls enough computers, they can use the infected computers to send more service requests than the system can handle. This will likely overwhelm the network and knock it offline, making the computers or an online service unavailable. The botmaster may also have the zombie (infected) computers send the target computer large amounts of random data that will use up the victim’s bandwidth or send hundreds of spam e-mails to a certain address.

A DDoS attack may go on for some time, as the owners of the infected computers are often not aware that their computers have been infected and in turn are being used to attack others. The machine will continue to infect others, adding to the army of computers that the botmaster controls.

When a botmaster is able to use multiple (hundreds or even thousands) of computers to flood a target system, it is often difficult identify the source of the attack. As the attack may be from a location far away, identification of the offender is made even more difficult. Because of this, a DDoS attack will go unsolved and the offender is never caught or punished. And because the attack is from so many sources, it becomes difficult to prevent the attacks.

Botnets can currently be purchased on the dark web, often for around $100. These are a type of computer malware that can be used to send large amounts of spam e-mails to others, steal data or information from computers, or to carry out DDoS attacks on other computers. Many different types of botnets are for sale on the dark web, making the malware available to just about anyone, whether it is an individual or group. With a botnet, a website or network can be shut down if a person or group is not pleased with the organization. They may simply disagree about the political message being sent and want to shut it down, or may be former employees who are seeking revenge for some reason.

DDoS attacks happen frequently. In 2007, Russian nationalists who were mad at Estonia after that country moved a Soviet war monument chose to launch a DDoS attack against the government sites of Estonia and Georgia, knocking them offline. In 2010, the hacking group Anonymous launched an attack against PayPal, Visa, and MasterCard after these organizations announced that they would not process financial donations given in support of WikiLeaks (Zetter, 2016). As a result of the attack, these sites were offline for about 8 hours, costing the company millions of dollars.

Anonymous attacked again in 2012, this time focusing on groups that supported the Stop Online Piracy Act (SOPA), including the U.S. Department of Justice, the FBI, the White House, the Motion Picture Association of America, the Recording Industry Association of America, Universal Music Group, and the Broadcast Music Inc. The group was able to take the websites offline for many hours. Anonymous members took their attack one step further by urging others who were opposed to the legislation to allow Anonymous to use their computers as a bot to further the attack.

A DDoS attack was carried out on the British Broadcasting Corporation (BBC) on New Year’s Eve in 2015 (January 2016). This attack was planned by the New

World Hacking, a group that also attacked Donald Trump's presidential campaign website on that same day. On April 1, 2016, Anonymous launched another DDoS attack on the presidential campaign websites belonging to Donald Trump. They sought to bring the websites for his hotel chain offline. Hackers also went after the website belonging to the Democratic candidate, Hillary Clinton.

Later in 2016, the servers of Dyn, a company that oversees a large portion of the internet domain name system (DNS), were under attack by a DDoS assault. This brought down Twitter, the *Guardian*, Netflix, CNN, and other sites. This attack was unusual because it relied on the "Internet of Things" devices such as digital cameras and DVR players (Woolf, 2016).

See also: Anonymous; Denial-of-Service Attack (DoS); Malware; Social Engineering

Further Reading

"Anonymous hacker's message to Congress on SOPA." 2012. Hackread, January 21, 2012. https://www.hackread.com/anonymous-hackers-message-to-congress-on-sopa/

Mirkovic, Jelena, Sven Dietrich, David Dittrich, and Peter Reiher. 2005. *Internet denial of service: Attack and defense mechanisms*. Upper Saddle River, NJ: Prentice-Hall.

Perlroth, Nicole. 2016. "Hackers used new weapons to disrupt major websites across U.S." *New York Times*, October 21, 2016. https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html

Woolf, Nicky. 2016. "DDoS attack that disrupted internet was largest of its kind in history, experts say." *The Guardian*, October 26, 2016. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

Yu, Shui. 2014. *Distributed denial of service attack and defense*. New York: Springer.

Zetter, Kim. 2016. "Hacker lexicon: What are DOS and DDOS attacks?" *Wired*, January 16, 2016. https://www.wired.com/2016/01/hacker-lexicon-what-aare-dos-and-ddos-attacks/

DOMAIN NAME SYSTEM CACHE POISONING

DNS cache poisoning is a type of cyberattack in which a cybercriminal sends a fake address for an internet domain into a DNS response system, where it is stored in the cache. If the server accepts the fake record, incorrect information is stored in the cache. This means that the DNS system has become "poisoned." Any future user requesting the IP address will be redirected and sent to the fake IP address that is controlled by the offender. The fake websites that users are sent to will appear to be the actual website but are actually fake ones set up by the offender to steal the victim's personal information.

A DNS associates domain names with IP addresses. They help to transmit e-mails and URLs that are read and understood by people and converted into data that can be read by computers. Over time a DNS will create a cache, or a collection of data that allows a person requesting data in the future to retrieve that information more quickly. A DNS server will cache information from other DNS servers; this way, it can use information that has already been gathered rather than gather it all over again. It makes the system more efficient. A cybercriminal relies on a vulnerability that may exist in the DNS software to attack a system. The offender may send a fake address for an internet domain into a DNS response to a system, where it is stored in the cache. If the server accepts the fake record, incorrect information is stored in the cache. This means that the DNS cache has become poisoned.

For example, a user may type into a search "nytimes.com" and end up at a site that appears to be the *New York Times* but is actually a fake site controlled by a cybercriminal. The victim may log into the site with their name and password, or even credit card information, but that information is being viewed by the offender.

A spoofing attack can also be directed at an e-mail system. In these attacks, an offender uses a fake record for an e-mail server that will redirect corporate e-mail to a fake e-mail address (Halley, 2008). This allows the offender to have access to all employee e-mails, including personal and corporate secrets.

These types of cyberattacks do not require sophisticated techniques, but they are very difficult to detect. They can be very damaging. They can often easily spread from one DNS server to another without the owner's knowledge. They have also been used to spread malware, including worms and viruses, to other systems. In some attacks, hundreds of people have ended up at a fake site.

Once discovered, the corrupted or poisoned cache must be cleaned so that future users will not be sent to the wrong site. It has been suggested that companies and organizations clear their caches often as a way to prevent a DNS cache poisoning attack.

See also: Spoofing

Further Reading

Delaney, Kevin J. 2005. "'Evil Twins' and 'Pharming': Hackers use two new tricks to steal online identities; scams are harder to detect." *Wall Street Journal*, May 17, 2005. https://www.wsj.com/articles/SB111628737022135214

Halley, Bob. 2008. "How DNS cache poisoning works." NetworkWorld, October 20, 2008. https://www.networkworld.com/article/2277316/tech-primers-how-dns-cache-poisoning-works.html

Hoffman, Chris. 2015. "What is DNS cache poisoning?" HowToGeek, January 9, 2015. https://www.howtogeek.com/161808/htg-explains-what-is=dns-cache-poisoning

DOXING

Doxing is the intentional, public disclosure of identifying information about someone (name, address, social security number, etc.). This primarily occurs on the internet. Those who dox another individual may obtain the identifying information in any number of ways, such as hacking. However, it is possible that the identifying information may be obtained in completely legal ways, such as obtaining it from public records.

Doxing can be seen as a harmless practice. Disclosing the identifying information of someone is not, per se, harmful. It is what others do with that information that can be harmful. For example, in the case of *McAdams v. Marquette University*, 2018 WI 88, John McAdams, a professor at Marquette University, took exception to the actions of Cheryl Abbate, a graduate student in philosophy at the university. During a Theory of Ethics course that Abbate was teaching in 2014, she apparently put a list of topics on the board—among which was gay rights—and told the class there was no need to discuss the listed topics, as everyone apparently agreed on them. A student approached Abbate after class and expressed their opinion that gay rights should have been a topic open for discussion. Abbate chastised the student, telling them they did not "have a right in [that] class to make homophobic comments." Abbate then informed the student they could drop the class.

Following this incident, McAdams posted about it on his blog, providing Abbate's name and a link to her personal website, which contained her contact information. In his blog post, McAdams criticized Abbate for using "a tactic typical among liberals," to wit, "[o]pinions with which they disagree are not merely wrong, and are not to be argued against on their merits, but are deemed 'offensive' and need to be shut up." Abbate filed a complaint against McAdams with the university. Abbate felt that McAdams was a "homophobic idiot" who was "insert[ing] his ugly face into [her] class business to try to scare her into silence."

After Abbate filed a complaint, the story began to get national attention. Abbate subsequently received several offensive and harassing communications. Marquette University suspended McAdams for a time. As a condition for returning to his professorial duties, the university required McAdams to write a letter to the university president's office expressing remorse for the harm he caused Abbate by publicly criticizing her and doxing her. He refused and instead filed a lawsuit against the university for breach of contract. The Wisconsin Supreme Court ultimately ordered the university to reinstate McAdams. In its ruling the court criticized Marquette University for "subject[ing] a tenured professor to discipline for writing something that triggered an adverse response from third parties over whom he has no control." As can be seen, the doxing itself it not necessarily what is harmful. Rather, it is what others do with the information—such as sending harassing e-mails—that can be harmful.

Consequences may extend beyond harassing communications. In 2008, WikiLeaks released the names and addresses of members of the British National Party, a far-right political party. The occupations of party members were released as well. This resulted in at least one party member being terminated from their place of employment (Chivers, 2017). In 2014, Zoe Quinn—an independent video game developer—had personal information unearthed by hackers following claims by her ex-boyfriend (Eron Gjoni) that she had sex with a video game journalist to improve the review of her game *Depression Quest*. This event marked the beginning of what is known as Gamergate—an unorganized movement whose purpose is not clearly defined but appears generally to push back against progressivism in video games. As a result of being doxed, Quinn received death threats and rape threats (Quinn, 2017). Other women, such as critic Anita Sarkeesian and game developer Brianna Wu, also were doxed as part of Gamergate. They also received death threats and rape threats. For all three women, these threats grew so severe that at some point, they had to flee their homes (McDonald, 2014).

Doxing can be additionally harmful when it misidentifies someone. This happened to Sunil Tripathi, a student at Brown University who went missing in 2013. Tripathi's family circulated his name and picture on social media in attempts to find him. Soon after, the Boston Marathon bombing occurred on April 15, 2013. Social media users suggested that Tripathi looked like one of the bombers. After this, his family received angry e-mails about Tripathi's supposed involvement, accusing them of harboring their fugitive brother and son. It was ultimately determined that Tripathi had not been involved. It was later discovered he had committed suicide (Lee, 2015). Nonetheless, harm had been inflicted on the family, and that harm could have escalated into something much worse—such as charges being brought against Tripathi and his family—had the actual suspects not been apprehended.

Doxing is increasingly becoming a political tool. Those who make statements or subscribe to views that are opposed by others face the threat of having their identity made public by those who oppose those statements or views. This appears to be what went on in the case of *McAdams v. Marquette University*, discussed above. McAdams did not approve of the views expressed by Abbate in her class (believing them to have a liberal bias), so he posted her contact information on his blog. This also happened with the protests in Charlottesville, Virginia, in 2017. Numerous white supremacists marched in town, holding torches. A number of those white supremacists were doxed. There are those who oppose the views held by white supremacist groups and feel that doxing is a valid way of holding those who have those views accountable to the public (Bowles, 2017).

By and large, doxing is not a crime. There are some limited instances in which it might be criminal. For example, it is a federal crime to make public the restricted personal information of certain people, such as jurors, witnesses, and officers of the court. Generally, if a criminal action is going to be pursued for doxing at all, it would have to be done under a state statute for harassing or something similar. Even then, there are rights citizens in the United States have under the Free Speech Clause of the First Amendment of the U.S. Constitution that would have to be considered and might ultimately prevent a prosecution from being successful. In the case of John McAdams, the Wisconsin Supreme Court ultimately held that his publishing of the graduate student's name and contact information was protected by the First Amendment. In short, it is difficult to hold those who dox legally responsible for the harm generated by their actions (Binder, 2018).

While it may be difficult to hold those who dox legally responsible, there are mechanisms online that may deter doxing. Some social media sites prohibit doxing in their terms of service. For example, Reddit prohibits the posting of personal information, including information that might be public. It does have an exception to this rule with regard to public figures (Reddit, 2018). Twitter does prohibit the posting of private information, but it does not prohibit the posting of public information (Twitter, 2018). Because social media companies are not state actors, they are not prohibited from blocking certain speech from their sites. Thus, there is no First Amendment violation if they prohibit doxing on their sites.

Although doxing primarily occurs on the internet, there are examples of doxing that occurred before the advent of the internet. Baseball umpire Don Denkinger's home address and phone number were broadcast by two disc jockeys from St. Louis after the St. Louis Cardinals lost in the World Series in 1985. Cardinals fans blamed the loss on Denkinger due to a missed call. Denkinger and his family received various threats, including one to burn down their home (Greene, 2015). In another incident, far-right activists in the United Kingdom posted the phone number of race relations campaigner Lord Herman Ouseley in public restrooms in London. He received numerous phone calls late at night as a result (Ellis, 2017).

There have been instances when news outlets have either doxed an individual or threatened to do so. It has led some to question why doxing is viewed differently when done by a news outlet as compared to a private individual and whether the two should be viewed differently (Ellis, 2017). One incident of doxing by a news outlet was carried out by the *Phoenix New Times*, a newspaper out of Phoenix, Arizona. The newspaper ran an article that published the home address of Sherriff Joe Arpaio, whom the newspaper has various disagreements with (Dougherty, 2004). In a 2017 incident, CNN was able to identify a Reddit user who had posted a GIF of Donald Trump beating someone who had a CNN logo in place of their head. The Reddit user's post history on the site included racist content. CNN did not post the user's personal information, in part because the user issued an apology for his racist post upon discovering that CNN knew his identity. However, CNN threatened to release the user's information should he ever post offensive content in the future (Kaczynski, 2017).

See also: Cyberbullying; Hacker and Hacking; Hacktivism; Privacy; Revenge Porn; Social Media; State Actor; Swatting; WikiLeaks

Further Reading

Binder, Nellie Veronika. 2018. "From the message board to the front door: Addressing the offline consequences of race- and gender-based doxxing and swatting." *Suffolk University Law Review* 55: 55–75.

Bowles, Nellie. 2017. "How 'doxxing' became a mainstream tool in the culture wars." *The New York Times*, August 30, 2017. https://www.nytimes.com/2017/08/30/technology/doxxing-protests.html

Chivers, Tom. 2017. "Wikileaks' 11 greatest stories." *The Telegraph*, March 8, 2017. https://www.telegraph.co.uk/news/0/wikileaks-greatest-ever-stories-scandals/

Dougherty, John. 2004. "Stick it to 'em." *Phoenix New Times*, July 8, 2004. https://www.phoenixnewtimes.com/news/stick-it-to-em-6428128

Ellis, Emma Grey. 2017. "Don't let the alt-right fool you: Journalism isn't doxing." *Wired*, July 7, 2017. https://www.wired.com/story/journalism-isnt-doxing-alt-right/

Greene, Dan. 2015. "After the call." *Sports Illustrated*. https://www.si.com/longform/2015/1985/world-series-cardinals-royals/index.html

Kaczynski, Andrew. 2017. "How CNN found the Reddit user behind the Trump wrestling GIF." *CNN*, July 7, 2017. https://www.cnn.com/2017/07/04/politics/kfile-reddit-user-trump-tweet/index.html

Lee, Traci G. 2015. "The real story of Sunil Tripathi, the Boston bomber who wasn't." *NBC News*, June 22, 2015. https://www.nbcnews.com/news/asian-america/wrongly-accused-boston-bombing-sunil-tripathys-story-now-being-told-n373141

McDonald, Soraya Nadia. 2014. "'Gamergate': Feminist video game critic Anita Sarkeesian cancels Utah lecture after threat." *Washington Post*, October 15, 2014. https://www.washingtonpost.com/news/morning-mix/wp/2014/10/15/gamergate-feminist-video-game-critic-anita-sarkeesian-cancels-utah-lecture-after-threat-citing-police-inability-to-prevent-concealed-weapons-at-event/?utm_term=.47212285ba0b

Quinn, Zoe. 2017. "What happened after GamerGate hacked me." *Time*, September 11, 2017. http://time.com/4927076/zoe-quinn-gamergate-doxxing-crash-override-excerpt/

Reddit. 2018. "Is posting someone's private or personal information okay?" Reddit. https://www.reddithelp.com/en/categories/rules-reporting/account-and-community-restrictions/posting-someones-private-or-personal

Twitter. 2018. "About private information on Twitter." Twitter. https://help.twitter.com/en/rules-and-policies/personal-information

DRAPER, JOHN (1943–)

Otherwise known as Cap'n Crunch, Draper was an original "phone phreak," an individual who studied telecommunications systems and public telephone networks, particularly audio frequencies (the clicks and beeps) that are used to provide services to customers, to understand how they worked and how they could be manipulated. Phone phreaks were able to make free phone calls and conference calls to each other as they shared what they knew. Eventually, many phone phreaks were arrested, and some were sent to jail, including Draper.

Draper's father was in the air force, and his family moved often. As a young boy, John searched for various electronic parts on the military bases where his father was stationed so he could build a radio station in his bedroom. When he was old enough, Draper joined the air force and became a radar technician. While stationed in Maine, he studied the phone system on the base and learned how to make free phone calls through a switchboard. When discharged from the military, Draper met others who were fascinated by the inner workings of telephones, including Joe Engressia. These individuals became known as "phone phreakers." Joe realized that he could bypass the long-distance system set up by Bell Telephone by whistling the correct tone. When he told Draper of his discovery, Draper soon realized that the toy whistle inside a box of Cap'n Crunch cereal made the same tone. When he blew the whistle, he could call anywhere for free. He once claimed that he was able to get President Richard Nixon on the phone to report a shortage of toilet paper.

In 1971, *Esquire* magazine published an article about phone phreaking that identified Draper and other phone phreaks. The author of the article, Ron Rosenbaum, explained that the phone phreakers, including Draper, were able to override the phone system and make telephone calls for free. The author went into detail about how the "little blue box" enabled a caller to make calls around the world without cost and without the call being traced and also brought up the possibility of using the blue boxes to break into the FBI's computer system. Not long after the article was published, Draper was arrested and charged with violating laws on wire fraud. He was sentenced to five months of probation. He was arrested again in 1976 and wasn't released until February of 1977. As an inmate, Draper used his radio to listen to the walkie-talkies of the prison guards. He provided the other inmates lessons in phone phreaking. Toward the end of his sentence, he was allowed to leave the prison during the day (his sentence was nights only). During the day, he wrote a word-processing program called Easy Writer.

When Draper was released in 1977, Apple cofounder Steve Wozniak hired him as a contractor. There he designed a device called a Blue Box that was able to identify phone signals and lines that allowed him to make free phone calls. Apple did not pursue the device because of the fear of negative publicity. When outsiders got ahold of the technology, they used it to harass offices or disrupt business.

Draper was sent back to prison for a parole violation and sent to Pennsylvania. While he was there, another inmate asked him for help in hacking into the telephone network. Draper thought he was an informer, so he provided false information. When the inmate was unable to make the calls, he physically attacked Draper and caused permanent damage to his vertebrae.

Following the failure of his business venture, Cap'n Software, Draper worked for several years in the late 1980s for Autodesk Inc., a San Rafael, California, company that makes design software. He was laid off when new management took over the company.

In 1987, law enforcement investigated Draper for a plot to forge tickets for the Bay Area Rapid Transit (the BART) in San Francisco. He pleaded guilty to lesser misdemeanor charges in 1988. This time, he was not sentenced to a corrections facility but instead to a diversion program.

In his later years, Draper has traveled to Australia and India, where he made a living earning money designing websites and writing computer code.

See also: Abene, Mark; Blankenship, Loyd, Timothy; Engressia, Josef Carl, Jr.

Further Reading

Draper, John and C. Wilson Fraser. 2018. *Beyond the little blue box*. Victoria, BC: FriesenPress.

Markoff, John. 2001. "The odyssey of a hacker: From outlaw to consultant." *New York Times*, January 29, 2001. https://www.nytimes.com/2001/01/29/business/the-odyssey-of-a-hacker-from-outlaw-to-consultant.html

Rhoads, Christopher. 2007. "The twilight years of Cap'n Crunch; Silicon Valley legend John Draper made his name with brains and pranks, before slipping to the margins; Three jail stints and the 'rave' scene." *Wall Street Journal*, January 13, 2007.

Rosenbaum, Ron. 1971. "Secrets of the little blue box." *Esquire* (October): 117–226. https://classic.esquire.com/article/1971/10/1/secrets-of-the-blue-box

Schneider, Howard. 2013. "Playing tricks on Ma Bell; Early hackers made free phone calls with a toy whistle and managed to reach the president on an unlisted hotline." *Wall Street Journal*, February 1, 2013. https://www.wsj.com/articles/SB10001424127887324039504578259861535539082

DREAD PIRATE ROBERTS (ULBRICHT, ROSS; 1984–)

Dread Pirate Roberts was the online name for the owner and operator of Silk Road, an online marketplace that operated on the dark web, where drugs and other items could be purchased. The online name was taken from the character of the same name in the book and movie *The Princess Bride* (1973, novel; 1987, film). The character wears a mask to protect his anonymity and also to hide the fact that Dread Pirate Roberts is not a person but rather a title that passes from person to person when the current Dread Pirate Roberts is ready to be done. The use of this name led many to believe that the Dread Pirate Roberts who ran Silk Road was not one person but a series of people (Bearman et al., 2015a). In 2013, Operation Marco Polo, a multiagency law enforcement investigation into Silk Road, discovered that Dread Pirate Roberts was Texas native Ross Ulbricht.

For Ulbricht, Silk Road was about cutting out government oversight from transactions he believed the government should not be involved in. To truly be able to do this, Ulbricht believed the transactions had to be anonymous. For this reason, the site conducted transactions using Bitcoin. Ulbricht and many users subscribed to libertarian ideology and saw Silk Road as an application of those ideals. This can be seen in the rules for Silk Road. Following libertarian ideology that people should have freedom to do what they like as long as it does not infringe on others' ability to do the same, Silk Road prohibited the sale of certain items that could only have been obtained by infringing on the freedom of others. This included items that had been stolen and child pornography (Bearman et al., 2015a, 2015b).

Following Operation Marco Polo, the FBI arrested Ulbricht in San Francisco in October 2013. On February 4, 2015, a jury found Ulbricht guilty of money laundering, computer hacking, conspiracy to traffic fraudulent identity documents, and conspiracy to traffic narcotics by means of the internet. On May 29, 2015, he was sentenced to life in prison at age 31 (Segall, 2015).

There are many who see Ulbricht as a martyr for a noble cause. Some of Ulbricht's family and friends have put together a website (freeross.org) to share Ulbricht's story as they see it. According to the website, Ulbricht created Silk Road, but not with specific designs to make it a drug-trafficking website. Rather, he intended it as a "free-market economic experiment" where buyers and sellers could maintain anonymity. It notes that Silk Road never told users specifically what to sell, though it did have prohibitions—as noted above—against selling items that would infringe on others' rights or involve victims (Free Ross Ulbricht, 2018). While it may not have told users what to sell, it appears Silk Road had a user's guide detailing how sellers could package drugs to avoid detection by narcotics canines and other detection devices that the postal service or other shipping companies might use (Bearman et al., 2015a). The website then details and criticizes several aspects of the criminal investigation against Ulbricht, such as the motivations of the officers involved and the overlooking (or perhaps covering up) of certain pieces of evidence (Free Ross Ulbricht, 2018). Two agents involved in the investigation—Agent Mark Force and Agent Shaun Bridges—were later convicted of stealing Bitcoin during the investigation (Raymond, 2017).

One of the controversial portions of the legal case against Ulbricht is the allegations of murders that Ulbricht allegedly paid for. One murder he is said to have paid for is that of Curtis Green, an employee of Silk Road who was arrested and was working with law enforcement. The arrangement to have Green killed was set up with Agent Force—one of the agents who was later convicted for stealing Bitcoin during this investigation—who was acting in an undercover capacity at the time. Agent Force staged pictures of Green being tortured and of Green's dead body, and these were sent to Ulbricht. Ulbricht allegedly paid Agent Force for carrying out the hit (Bearman et al., 2015a). Five other murders that Ulbricht is alleged to have paid for appear to have been a scheme orchestrated against Ulbricht to defraud him of money, with none of the murders actually taking place (Bearman et al., 2015b). While Ulbricht was not convicted for these murders-for-hire, they were mentioned during his trial on other charges and appear to have been considered by the judge when sentencing Ulbricht on those other charges (Segall, 2015). Ulbricht appealed his sentence, claiming it was unreasonable, but the appellate court upheld the sentence.

In keeping with the fictional character behind the name, the "Dread Pirate Roberts" moniker was adopted by another after Ulbricht was arrested. Following the shutdown of Silk Road in 2013 as part of Operation Marco Polo, the website reopened shortly thereafter as Silk Road 2.0. This iteration of the site was founded by Thomas White. White had gone by the name StExo on the original Silk Road site but switched to the name Dread Pirate Roberts 2 with the founding of Silk Road 2.0 (Cox, 2019). Silk Road 2.0 was short-lived, staying in operation only a year. While running the site, White directed hackers to attack other dark web marketplaces, such as Agora, TorMarket, and Sheep Marketplace (Cox, 2016). While it was in operation, it is estimated that Silk Road 2.0 generated $8 million in sales a month. White and the other owners of Silk Road 2.0 took between 4 and 8 percent of each transaction that was conducted through the site. White claims to have not kept much of the profit for himself, instead passing it on to the Tor Project and other organizations and charities (Cox, 2016). In 2014, Silk Road 2.0 was shut down as part of Operation Onymous (Cook, 2014). As part of that investigation, White was arrested by law enforcement in the United Kingdom. He ultimately pleaded guilty to drug trafficking, money laundering, and making indecent images of children. He was sentenced in 2019, receiving a sentence of over five years in prison (Cox, 2019).

See also: Bitcoin; Money Laundering; Operation Marco Polo; Privacy; Silk Road; Tor (The Onion Router)

Further Reading

Bearman, Joshuah, Joshua Davis, and Steven Leckart. 2015a. "The rise & fall of Silk Road, part 1." *Wired*. https://www.wired.com/2015/04/silk-road-1/

Bearman, Joshuah, Joshua Davis, and Steven Leckart. 2015b. "The rise & fall of Silk Road, part 2." *Wired*. https://www.wired.com/2015/05/silk-road-2/

Cook, James. 2014. "FBI arrests former SpaceX employee, alleging he ran the 'deep web' drug marketplace Silk Road 2.0." *Business Insider*, November 6, 2014. https://www.businessinsider.com/fbi-silk-road-seized-arrests-2014-11

Cox, Joseph. 2016. "The secret life of a Silk Road 2.0 mastermind." Motherboard, March 10, 2016. https://motherboard.vice.com/en_us/article/3dad83/the-secret-life-of-a-silk-road-20-mastermind

Cox, Joseph. 2019. “Silk Road 2 founder Dread Pirate Roberts 2 caught, jailed for 5 years.” Motherboard, April 12, 2019. https://motherboard.vice.com/en_us/article/9kx59a/silk-road-2-founder-dread-pirate-roberts-2-caught-jailed-for-5-years

Free Ross Ulbricht. 2018. “Railroaded: The targeting and caging of Ross Ulbricht.” Free Ross Ulbricht. https://freeross.org/railroaded/.

Raymond, Nate. 2017. “Ex-agent in Silk Road probe gets more prison time for bitcoin theft.” *Reuters*, November 7, 2017. https://www.reuters.com/article/us-usa-cyber-silkroad/ex-agent-in-silk-road-probe-gets-more-prison-time-for-bitcoin-theft-idUSKBN1D804H

Segall, Laurie. 2015. “Silk Road’s Ross Ulbricht sentenced to life.” CNN, May 29, 2015. https://money.cnn.com/2015/05/29/technology/silk-road-ross-ulbricht-prison-sentence/index.html

DREAMBOARD

Dreamboard was the name of a global community of pedophiles that shared images of child abuse. It was an online, private, international network of an estimated 600 members who promoted acts of pedophilia. They sought to exchange massive amounts of graphic, pornographic images of adults molesting children, some of whom were infants. They had amassed a private collection of images of child sexual (often violent) abuse. The children appeared to be the subjects of both physical and emotional distress. Many were in obvious pain and crying.

Many of the group members claimed to believe that sexual abuse of children should not be a crime. Instead, the members described their actions as more of a hobby than a criminal offense. To become an official member of Dreamboard, a person is required to upload images of children under the age of 12 in pornographic acts at least once every 50 days. The content and quality of the material was critical. Images of adults having violent sexual intercourse with young children were given more value than other images.

Once a person became a member, they had to continue to create and upload new images in order to remain a member in good standing. If an individual did not continue to upload images, they could be removed as a member, and their access to the network was removed. This process maintained a continuous stream of new images of child molestation.

Given that process, the group established different types of memberships in Dreamboard. The first category was the “Super VIP,” recognizing members who continually obtained new images, often by molesting children themselves, and then uploading those images. The second type of membership was VIP, which included those members trusted by the organization. The third type included the regular members, who were given access to view a limited number of photos.

Dreamboard also created rules for its members to obey. All members were required to regularly upload new images of children engaging in sexual activity. Members had to post their images to different categories, depending on the type of image or abuse.

On August 3, 2009, law enforcement officials from the Homeland Security Investigations team from U.S. Immigration and Customs Enforcement (ICE) and the Department of Justice, along with officials from Eurojust (the European

Union's Judicial Cooperation Unit) and other international law enforcement agencies, established Operation Delego to investigate Dreamboard. The investigation quickly became the largest investigation of child abuse and exploitation in the history of the United States. The investigation was an international investigation that involved law enforcement from multiple international agencies.

The law enforcement agents soon discovered that the members of Dreamboard used aliases. The members used an encrypted password that only members possessed. They also used proxy servers as a way to hide their location and identity. Nonetheless, on August 3, 2011, U.S. Attorney General Eric Holder and Secretary of the Department of Homeland Security (DHS) Janet Napolitano announced criminal charges against 72 members of Dreamboard. The defendants were found in five continents and 14 countries, including Canada, the Netherlands, Philippines, Serbia, Switzerland, Germany, France, and others. Officials also found that another 500 people were participating in Dreamboard.

As a result of the investigation, active Dreamboard member John Wyes (also known as Bones) was found guilty of one count of engaging in a child exploitation enterprise, one count of conspiracy to advertise child pornography, and one count of conspiracy to distribute child pornography. The evidence gathered by law enforcement indicated that Wyss helped to produce images of child pornography, including a video that showed adults were having sexual relations with children. He was sentenced to life in prison.

Another member, David Ettlinger (aka ee1) from Massachusetts, was a former elementary school teacher who pleaded guilty to one count of engaging in a child exploitation enterprise. He was sentenced to 45 years in prison, followed by a lifetime on supervised release. The investigation also charged eight other individuals, whose prison sentences ranged from 17 years to life.

See also: Child Pornography

Further Reading

Frieden, Terry. 2011. "72 charged in online global child porn ring." CNN, August 3, 2011. www.cnn.com/2011/CRIME/08/03/us.child.porn.ring/index.html

"Operation Delego: Dreamboard child sex ring bust nets 72 arrests in U.S., Canada, France, Germany." 2011. *HuffPost*, August 3, 2011. https://www.huffingtonpost.ca/2011/08/03/operation-delego-dreamboard-child-sex-ring_n_917633.html

Perez, Evan. 2011. "U.S. charges 72 in child-pornography probe." *Wall Street Journal*, August 3, 2011. https://www.wsj.com/articles/SB10001424053111903366504576486253988839230

Savage, Charlie. 2011. "Network that preyed on children is broken." *New York Times*, August 3, 2011. https://www.nytimes.com/2011/08/04/us/04porn.html

DRINK OR DIE

Drink or Die (DoD) was a group of mostly undergraduate students who formed a software piracy organization in the 1990s. They claimed to be the first group to distribute a perfect copy of a pirated (stolen) software product. The group was able to release Windows 95 two weeks before Microsoft officially released the operating software. They also reproduced and distributed over $50 million worth of pirated software, games, movies, and music. The group did not operate for profit but instead wanted to be known for "robbing from the rich to give to the poor." Some members simply sought out the challenge. In 1993, students known online as "Jimmy Jamez" (also called "the deviator") and "CyberAngel" formed the group in Moscow, Russia. By 1995, the group contained members from around the world.

The group disbanded in 2000s after U.S. Customs initiated Operation Buccaneer, a 14-month undercover operation that led to a series of international raids, with many members arrested. Customs agents had been provided with critical information about the group by one its members, James Cudney (Bcrea8tiv). He gathered information on the individual members' activities and passed that along to officials. Law enforcement in 12 countries, including the United States, Sweden, Australia, Finland, Norway, and England, executed over 100 search warrants simultaneously, making 65 arrests. By the time law enforcement carried out the raids, the organization was largely out of business. Customs agents described the members as being from diverse backgrounds, including successful businessmen who worked in major corporations, universities, high-tech companies, and the government.

One member, Hew Raymond Griffiths, aka Bandido, was a resident of Australia. Griffiths was eventually extradited to the United States to face criminal charges for his activities. He served 15 months in jail after serving three years in Australia. Philadelphia resident John Sankus Jr. was convicted in 2002 and sentenced to 46 months in federal prison. Christopher Tresco (aka BigRar), from Massachusetts, pleaded guilty in 2002 in Federal Court of using his employer's computer to distribute copyrighted material. He worked at the Massachusetts Institute of Technology (MIT) in the economics department. Barry Erickson, from Oregon, was sentenced to 33 months in prison after pleading guilty to one count of conspiracy to commit criminal copyright infringement, a felony offense. Erickson was able to provide Symantec software to the group that had its copyright-protection removed.

Alex Bell, from Grays, Essex (England), was sent to prison for two and a half years for conspiracy to defraud; Steven Dowd, from Newton-le-Willows, Merseyside (England), was charged with the same crime and also sent to prison for two years. Andrew Eardley from London and Mark Vent of England pleaded guilty to software piracy charges. Vent was sentenced to 18 months and Eardly was given an 18-month sentence that was suspended.

See also: Copyright Infringement

Further Reading

"Arrests uncover global software piracy ring." 2001. *The Guardian*, December 12, 2001. https://www.theguardian.com/technology/2001/dec/12/piracy.news

Grabosky, Peter. 2007. "The internet, technology and organized crime." *Asian Journal of Criminology* 2, 2: 145–161.

Manjoo, Farhad Manijoof. 2001. “Were Drink or Die raids overkill?” *Wired*, December 13, 2001. https://www.wired.com/2001/12/were-drinkordie-raids-overkill/.

Summers, Chris. 2005. “The pirates with no profit motive.” BBC News, May 6, 2005. http://news.bbc.co.uk/2/hi/technology/4205559.stm

DRUG TRAFFICKING

Drug trafficking is the illegal commercial distribution of controlled substances. It encompasses all activities that take place in a commercial chain, including the manufacture of illegal drugs, the transportation of illegal drugs, and the ultimate sale of illegal drugs. Worldwide, between 6,000 and 8,000 tons of marijuana are seized annually, a similar amount of cocaine seized annually, and roughly 2,000 tons of opioids seized annually (United Nations Office on Drugs and Crime, 2017). In the United States alone, the federal government annually seizes millions of pounds of marijuana and thousands of pounds of heroin, cocaine, and methamphetamine (United States Customs and Border Protection, 2018; United States Drug Enforcement Administration, 2018).

Drug trafficking itself is not a cybercrime. However, drug trafficking can be accomplished through cyber means. Certain websites, such as Silk Road, have been used to arrange and facilitate the purchase of illegal drugs. Purchases via websites like Silk Road often involve payment in the form of cryptocurrency, such as Bitcoin. Because cryptocurrency transactions do not directly include the identity of the parties involved, the use of cryptocurrency can make these financial transactions difficult to trace.

One piece of evidence that law enforcement looks for when conducting drug interdiction is the presence of large sums of cash. Those who sell drugs are not going to accept payment in the form of personal check or credit card, as those transactions can be traced back to them. Traditionally, that has left cash as the only feasible option. Thus, when an individual is found to be in possession of a large sum of cash, and the owner of that cash cannot provide a reasonable explanation as to where the cash came from, that is viewed as circumstantial evidence that the person is involved in drug trafficking.

With the emergence of technology that allows people to exchange money in a less-visible, less-traceable way, drug traffickers are able to avoid carrying large sums of cash, such as using cryptocurrencies. Another method employed is the use of prepaid credit cards. Drug traffickers can place thousands of dollars on one prepaid credit card (the exact amount will depend on the rules of the credit card company whose card is being used), and that card can either be sent through the mail or inconspicuously placed in the drug trafficker’s wallet. Not only do these methods eliminate a potential source of evidence against drug traffickers in a criminal case, but they can also deprive the government of the opportunity to seize the money for civil forfeiture proceedings.

There are other ways drug traffickers use technology. Another piece of evidence that drug interdiction officers look for when investigating someone suspected of trafficking drugs is cell phones. Cell phones can contain a wealth of information for law enforcement. The cell phone of a drug trafficker may contain the contact information of other individuals involved in the drug trafficking network. This helps law enforcement piece together distribution networks and to identify new individuals involved in drug trafficking. If a drug trafficker is caught in the act of transporting drugs, it is possible for law enforcement to ascertain the identity of the intended recipient. In such instances, if law enforcement is able to act quickly, they may be able to use the information from a cell phone to pose as the apprehended drug trafficker and set up a meeting with the intended recipient of the drugs, resulting in additional arrests.

Knowing this, drug traffickers often utilize programs that allow their cellphones to be wiped clean from a remote location. In fact, many major cell phone and software companies provide programs that will allow a cell phone to be remotely wiped, including Apple, Google, and Microsoft (Pinola, 2017). Using a program like this would deprive law enforcement of any information they might otherwise be able to obtain. A drug trafficker can have a friend wipe the phone clean from a computer if the drug trafficker is caught and arrested. A friend might be alerted by the drug trafficker directly, just prior to being pulled over by law enforcement. There might also be a dead man's switch set up, whereby the friend will remotely wipe the phone if they have not heard from the drug trafficker for a predetermined amount of time.

Law enforcement has responded to the use of computer applications to wipe cell phones clean. If a cell phone is seized as evidence in a drug trafficking case, the phone will sometimes be stored in a Faraday bag. A Faraday bag is a fabric bag lined with a metal, such as aluminum, that is designed to block cell phone signals from reaching the inside of the bag. The name of these bags comes from Michael Faraday, a British scientist and inventor of the Faraday cage. A Faraday cage operates in the same was as a Faraday bag, using a metal enclosure to block out electromagnetic interference. By storing a cell phone in a Faraday bag, all incoming cell phone signals are blocked, preventing the contents of the phone from being deleted remotely. The phone must then be taken to an evidence room that likewise blocks out cell phone signals (a type of Faraday cage) before it is removed from the Faraday bag.

While it might be physically possible for law enforcement to look at the cell phone of a suspected drug trafficker before the contents are able to be deleted remotely, law enforcement officers in the United States are required to obtain a search warrant before legally being able to do so (*Riley v. California*, 134 S.Ct. 2473 (2014)). In the amount of time it takes to obtain a search warrant, a cellphone could easily be wiped clean remotely. This makes the presence of Faraday bags as a law enforcement tool all the more valuable.

See also: Cryptocurrency; Silk Road

Further Reading

Pinola, Melanie. 2017. "Install or enable remote wipe on your smartphone now." *Lifewire*, March 1, 2017. https://www.lifewire.com/install-or-enable-remote-wipe-on-your-smartphone-2377851

United Nations Office on Drugs and Crime. 2017. *World Drug Report 2017*. New York: United Nations.

United States Customs and Border Protection. 2018. "CBP enforcement statistics FY2018." https://www.cbp.gov/newsroom/stats/cbp-enforcement-statistics#

United States Drug Enforcement Administration. 2018. "Domestic drug data." https://www.dea.gov/domestic-drug-data

DUMPSTER DIVING

Cybercriminals use a variety of techniques to locate information that they can use to carry out an attack on another computer network. One of those methods is called "dumpster diving." This can occur when a person digs through a company's or individual person's trash bins or dumpster to find notes written on paper or other information that has been discarded. This can include names, phone numbers, printed e-mails, interoffice memos, or any discarded documents that can then be used by the offender to gain access to websites and steal information.

In the cyber world, this term can also apply to looking at relevant information located online about an individual or organization, including employee contact information, calendars with upcoming events, bank statements or financial records, health reports, or other basic information about a company. A cybercriminal can then use social engineering techniques (sending realistic but fake e-mails to employees) to collect data about an employee or a group of employees. The offender is able to then impersonate that employee to gain access to their files.

Hackers often find information from an employee who loses a flash drive or throws it away without erasing the information from it. In some cases, an angry employee will download information from the company onto a flash drive and remove it from the office. Cybercriminals also find old laptops and computers that are being thrown away before the hard drive is cleaned (or the data is still retrievable). This can be a good source of information.

In order to prevent dumpster diving, all trash should be shredded before being thrown away. Employees should also be aware of the threat of dumpster diving so they do not throw potentially damaging information in the trash where others may see it. Companies should also consider disk-wiping software that can be used prior to disposing of a system. Another option is encryption where data is coded and can only be read by someone who has a decoding key. Insider data theft can be limited by using software that detects when a foreign flash drive is inserted into a computer. Some companies limit what types of files an employee can download.

In some cases, hackers can get a lot of personal or damaging information very quickly. There is a substantial amount of information thrown into the trash each day that includes sensitive information. It is imperative that individuals and companies realize that so that precautions can be taken to prevent information from being stolen.

See also: Identity Theft; Personally Identifying Information

Further Reading

Long, Johnny. 2008. *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing*. Rockland, MA: Syngress.

Reitman, Janet. 2002. "Cyber dudes to the rescue." *Los Angeles Times*, November 17, 2002. http://articles.latimes.com/2002/nov/17/magazine/tm-cyber46

Scheier, Robert L. 2007. "Dumpster-diving for e-data." Computerworld, July 18, 2007. https://www.computerworld.com/article/2542491/enterprise-applications/dumpster-diving-for-e-data.html

E

ECONOMY, EFFECTS ON

Cybercrime negatively affects the economy. It has been estimated that cybercrime costs $6 trillion annually (Eubanks, 2017). There are several ways cybercrime affects the economy. One of those ways is through financial crimes. Financial crimes compose a significant amount of the cybercrime committed. Financial crimes can be committed against both consumers and businesses. The direct loss to consumers from financial cybercrimes is substantial. Based on complaints made to the FBI, victims of financial cybercrimes lost hundreds of millions of dollars in 2017. The most common complaint received by the FBI was for failure to receive goods paid for or failing to receive payments entitled to—a total of 84,079 complaints resulting in over $141 million in loss to the victims. Another 23,135 victims indicated they had been defrauded into overpaying for a good or service, resulting in a loss of over $53 million (Federal Bureau of Investigation, 2018).

Businesses suffer direct loss from cybercrime as well. Any cybercrime committed against a business that results in economic loss would arguably have an impact on the economy. This is because a business must take those losses into consideration when planning budgets, and this in turn can impact what that business charges for their goods and services, what that business pays their employees, and so on. Likewise, the cost of increased security to prevent those losses must be taken into consideration—an industry that is expected to reach $170 billion by the year 2020 (Better Business Bureau, 2017). Financial crimes committed against a business create a direct loss, and some businesses are specifically targeted for this purpose. Financial institutions tend to be targeted much more frequently—300 times more—than other businesses. This led to a loss of $16.8 billion to financial institutions in 2017 (Mirchandani, 2018). Data breaches also result in a loss for an attacked business. It is estimated that an average data breach can cost a company millions of dollars to address (Eubanks, 2017). Although the losses may not be as large comparatively, small businesses are also targeted by cybercriminals. It is estimated that the average loss resulting from a cyberattack on a small business is just shy of $80,000 (Better Business Bureau, 2017).

One cybercrime that particularly affects the economy is intellectual property theft. It has been estimated that the annual amount of U.S. intellectual property stolen is up to $600 billion (Commission on the Theft of American Intellectual Property, 2017). Not all intellectual property theft would be considered cybercrime. The production and sale of counterfeit goods, for example, would be considered intellectual property theft. Looking at just the intellectual property theft that would be considered cybercrime (illegal downloading of movies, music, software, etc.), the annual amount lost is over $200 billion (Business Action to Stop Counterfeiting and Piracy and International Trademark Association, 2016). It is not just sellers of intellectual property that are affected but also those who stream intellectual property for a monthly fee, such as Netflix, Amazon, and Hulu. It is estimated that intellectual property theft from such streaming services will result in a loss of over $50 billion between 2016 and 2022 (Clarke, 2017). One of the things that sets intellectual property theft apart from other cybercrimes is the fact that many people engage in intellectual property theft. A survey conducted in the United Kingdom found that 60 percent of people had illegally downloaded or streamed intellectual property (Music Business Worldwide, 2018).

Direct losses are not the only losses that have an impact on the economy. There are several indirect losses from cybercrime that can impact the economy as well. For businesses that suffer a data breach that results in customer information being stolen, businesses face the potential of lawsuits from those customers. Target reached a settlement to pay $18.7 million as a result of a data breach it suffered (Eubanks, 2017). Sony and Home Depot did the same for data breaches they suffered, agreeing to pay out $15 million and $19.5 million, respectively (Armerding, 2018).

Intellectual property theft can result in indirect losses as well. Intellectual property theft inflicts the direct loss of unrecognized revenue on businesses. However, that unrecognized revenue can have compound effects. Lowered revenue can lead to lowered production by a company. This in turn can lead to fewer employment opportunities offered by that company, and a decrease in the amount of goods and services purchased by that company from other companies. Those other companies then face the same problem: lowered revenue leading to lower employment opportunities, etc. (Siwek, 2007). Additionally, intellectual property theft inflicts an indirect loss on governments in the form of lost tax revenue. One report in 2007 estimated that the loss to the U.S. federal, state, and local governments was $422 million annually (Siwek, 2007). Another report in 2016 estimated the global loss of tax revenues due to intellectual property theft to be $130 billion annually (Business Action to Stop Counterfeiting and Piracy and International Trademark Association, 2016).

Another indirect loss to businesses resulting from cyberattacks is the potential drop in consumer confidence that business may suffer. Several studies have found that when a business suffers some form of cyberattack, it negatively impacts the value of the business's stock and the overall valuation of the business (Bose and Leung, 2014; Goel and Shawky, 2009; Pirounias et al., 2014; Spanos and Angelis, 2014).

The losses suffered by businesses can ultimately affect consumers as well. As noted above, a business that suffers a loss may increase the cost of its goods and services as a means of compensating for that loss. Thus, law-abiding consumers may have to pay more for goods and services due to the prevalence of cybercrime. Even companies that do not suffer a loss from an attack still have to pay to have cyber security in place, and that cost may be passed on to consumers as well. Consumers are can be similarly impacted by unrecognized tax revenue resulting from intellectual property theft. If a government does not receive tax revenue from an expected source, it may resort to collecting it another way, with law-abiding consumers potentially shouldering that cost as well.

See also: Copyright Infringement; Entertainment, Effects on; Federal Bureau of Investigation; Financial Crimes

Further Reading

Armerding, Taylor. 2018. "The 18 biggest data breaches of the 21st century." *CSO*, December 20, 2018. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Better Business Bureau. 2017. "2017 State of cybersecurity among small businesses in North America." https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf

Bose, Indranil, and Alvin Chung Man Leung. 2014. "Do phishing alerts impact global corporations? A firm value analysis." *Decision Support Systems* 64: 67–78.

Business Action to Stop Counterfeiting and Piracy and International Trademark Association. 2016. "The economic impacts of counterfeiting and piracy." https://cdn.iccwbo.org/content/uploads/sites/3/2017/02/ICC-BASCAP-Frontier-report-2016.pdf

Clarke, Stewart. 2017. "Piracy set to cost streaming players more than $50 billion, study says." *Variety*, October 30, 2017. https://variety.com/2017/tv/news/piracy-cost-streaming-players-over-50-billion-1202602184/

Commission on the Theft of American Intellectual Property. 2017. "Update to the IP Commission Report." http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf

Eubanks, Nick. 2017. "The true cost of cybercrime for businesses." *Forbes*, July 13, 2017. https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#5af85ab24947

Federal Bureau of Investigation. 2018. "2017 internet crime report." https://pdf.ic3.gov/2017_IC3Report.pdf

Goel, Sanjay, and Hany A. Shawky. 2009. "Estimating the market impact of security breach announcements on firm values." *Information & Management* 46: 404–410.

Mirchandani, Bhakti. 2018. "Laughing all the way to the bank: Cybercriminals targeting U.S. financial institutions." *Forbes*, August 28, 2018. https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#2f4ac5b66e90

Music Business Worldwide. 2018. "83% of people who pirate music, film and TV tried to find it legally first, says survey." Music Business Worldwide, June 6, 2018. https://www.musicbusinessworldwide.com/83-of-people-who-pirate-music-film-and-tv-tried-to-find-it-legally-first-says-survey/

Pirounias, Sotirios, Dimitrios Mermigas, and Constantinos Patsakis. 2014. "The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study." *Journal of Information Security and Applications* 19: 257–271.

Siwek, Stephen E. 2007. "Reducing government consumption, increasing personal wealth." Institute for Policy Innovation. https://www.riaa.com/wp-content/uploads/2015/09/20120515_SoundRecordingPiracy.pdf

Spanos, Georgios, and Lefteris Angelis. 2016. "The impact of information security events to the stock market: A systematic literature review." *Computers & Security* 58: 216–229.

EINSTEIN

Einstein is a computer security program created by the DHS for two reasons. The first goal was to detect and then block cyberattacks that are aimed at computer networks found in federal agencies. The second goal was to allow DHS to use any threat information about a possible cyberattack that was discovered in one agency to help protect all other federal agencies and the private sector as well. The U.S. Computer Emergency Readiness Team (US-CERT), part of DHS's National Cyber Security Division, developed the software in 2003.

There were two phases to the Einstein program. The first phase monitored and looked for any changes or unusual patterns in the internet traffic surrounding the agency. To do this, past records were analyzed as a way to identify any possible malicious activity or to detect intrusions. The second phase, Einstein 2, focused more on the detection of suspicious activity or intrusions that had the potential to be harmful. The program relied on patterns from previous attacks, and then used that information to identify similar digital fingerprints. Together, it was hoped that Phases 1 and 2 would help experts detect potential cyberattacks before they happen. Phase 3 of the program would use the information gathered about a possible cyberoffense and block it before it could do any harm. It would examine the content of e-mails that are sent over government computer networks.

If any legitimate information about possible threats were identified through the process, DHS was to share the information with other departments and agencies and other partners in an effort to prevent cyberattacks. All agencies who participated in the program were required to sign a memorandum of understanding that outlined the level of participation. It was not adopted by all federal agencies. As of 2005, only three agencies had deployed the Einstein program. The procedures for sharing of information and for creating a unified response were unclear.

After President Barack Obama described the protection of computer networks as a national priority in 2011, he proposed a new program dubbed Einstein 3 (Obama, 2011). This was to shift the attention to the safety of the computer networks found in the private sector. The thrust of this program involved telecommunications companies that would monitor e-mails and other online activities through a box that would search for codes that appeared to be intended to compromise networks in same fashion. One critical issue surrounded methods to protect the privacy of all users. Another point of contention was the role that the National Security Agency (NSA) would have in reviewing and collecting data.

An analysis of the program by the General Accountability Office (GAO) showed that there were weaknesses with the Einstein program such that any information gathered from it were marginal. The GAO recommended that changes were needed for it to work properly. GAO analysts tested 489 known vulnerabilities but Einstein only detected about 29 of them, which is only a 6 percent success rate. In June 2015, a computer breach at the U.S. Office of Personnel Management quickly proved that the Einstein program failed to prevent hackers from accessing personal information on over 21 million federal employees. To date, Einstein has not stopped many of the more sophisticated and unknown attacks on government databases. Because the program relies on patterns found in past attacks, a new attack with new fingerprints will not be detected.

Another problem with the new program is that it does not identify criminals hacking into the networks of federal agencies using stolen passwords or other credentials. This is a problem, given that cybercrime experts have been able to locate the login credentials for approximately 50 federal agencies online. As of 2014, DHS reportedly spent over $500 million on the development and implementation of Einstein 1 and 2.

See also: Cybersecurity; Cyberterrorism; Prevention; United States Cyber Command

Further Reading

Chabrow, Eric. 2010. "Einstein presents big challenge to US-CERT." GovInfosecurity, June 22, 2010. http://www.govinfosecurity.com/einstein-presents-big-challenge-to-us-cert-a-2677.

Goode, Brendan. 2013. "Privacy impact assessment for Einstein3-Accelerated." U.S. Department of Homeland Security, April 19, 2013. https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf

Nakashima, Ellen. 2009. "DHS cybersecurity plan will involve NSA, telecoms." *Washington Post*, July 3, 2009. www.washingtonpost.com/wp-dyn/content/article/2009/07/02/AR2009070202771.html

Obama, Barack. 2011. "Fact sheet: Cybersecurity legislative proposal." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, May 12, 2011. https://www.presidency.ucsb.edu/node/323567

Paletta, Damian. 2015. "Breached network's security is criticized. System that failed to prevent millions of sensitive government files from being hacked is largely unable to stop the most sophisticated attacks." *Wall Street Journal*, June 23, 2015. https://www.wsj.com/articles/breached-networks-security-is-criticized-1435103680

Radack, Jesselyn. 2009. "Cyber overkill; A project to safeguard governmental computers, run by the NSA, is too big a threat to Americans' privacy." *Los Angeles Times*, July 14, 2009. http://articles.latimes.com/2009/jul/14/opinion/oe-radack14.

ELECTRONIC FRONTIER FOUNDATION

The Electronic Frontier Foundation (EFF) is a 501(c)(3) organization based in San Francisco, California, that works to ensure the privacy of those who use the internet. Originally, the nonprofit organization was founded in 1990 in Cambridge, Massachusetts, after the U.S. Secret Service tracked a document that had been illegally copied from a computer at BellSouth. The document described how the 911 emergency phone system worked. One of the people who allegedly possessed a copy of the document was Steve Jackson, a systems operator of a book publisher in Austin, Texas. The Secret Service seized all of the electronic equipment and copies of an upcoming book from his premises and then refused to return his property.

It was not long before Jackson had to lay off about half of his employees. When the Secret Service was unable to find any copies of the document on Jackson's computers, they returned his property. The data on the computers had been accessed and much of it deleted. Jackson's business was almost ruined. Jackson had a difficult time finding people to help him fight the raids until he met up with others who agreed that Jackson's privacy rights had been violated. Some people got together and decided to form a group to protect civil liberties of those who use technology. One of the forming members was John Perry Barlow, a lyricist for the Grateful Dead, a longtime advocate of online privacy.

Members of the group agree that individual rights and freedoms should not be blocked when it comes to the use of technology. Members seek to guarantee freedom of speech and oppose surveillance of online activities. They believe in the right of users to be able to communicate freely and privately through technology. They oppose policies that attempt to put limits on online speech, or that increase government surveillance of internet use. They support the use of open source software, research into security measures, and increased use of file sharing techniques. They support the development of software that can protect individual privacy and online security. EFF also has an international team that works for privacy and free speech in international arenas.

The EFF has become a legal advocacy group that agrees to work on lawsuits that challenge organizations that seek to limit a user's privacy. They help to provide funds for legal defenses in court. For example, in 2004, Ludlow Music, publisher of the Woody Guthrie song "This Land Is Your Land," filed a suit against JibJab Media, who used the song as a parody for the election being held that year. EFF, representing JibJab, argued that JibJab's version of the song was not covered by copyright laws because the parody was directed at the election rather than the song. The groups involved came to an out-of-court agreement.

In 2006, members of the group filed a class-action lawsuit against AT&T when it discovered that the company was working alongside members of the George W. Bush administration to support wiretapping of phones without a warrant.

Another case that the EFF provided assistance was *Bernstein v. U.S. Department of Justice* (922 F. Supp. 1426). Here, the plaintiff, Daniel J. Bernstein, was a PhD candidate student who developed an encryption code and wanted to publish it. The law at the time prohibited him from doing that. The EFF filed a lawsuit against the Department of Justice. The court decided that software code was protected under the First Amendment and that Bernstein was permitted to publish it.

Members of the EFF provided help in *MGM v. Grokster, LTD* (545 U.S. 913). The defendant, Grokster, Ltd., was a P2P (peer-to-peer) file sharing group. MGM, a movie production group, and 27 other entertainment companies filed a lawsuit to prevent Grokster from sharing pirated copies of movies. Here, the court decided that Grokster could be sued for violating copyright laws.

In *ACLU v. Reno II* (521 U.S. 844), EFF members sought to protect an individual's right to post certain materials online. The case was centered on the Communications Decency Act that made it illegal to publish certain content online. Supporters of the law sought to protect youth from viewing explicit material online. The ACLU claimed that some provisions of the act were unconstitutional and sought to prevent the government from enforcing some of the laws. The Supreme Court decided that online speech should be protected by the First Amendment, and that this law violated the amendment.

See also: Blankenship, Loyd; Encryption; Secret Service

Further Reading

Dwoskin, Elizabeth. 2015. "'Do not track' compromise is pitched: Electronic Frontier Foundation unveils a code of conduct for online publishers." *Los Angeles Times*, August 5, 2015. https://www.wsj.com/articles/do-not-track-compromise-is-pitched-1438821048

Electronic Frontier Foundation. 2019. https://www.eff.org/about

"Suit settled over political parody." *Los Angeles Times*, August 26, 2004. http://articles.latimes.com/2004/aug/26/business/fi-woody26

Timberg, Craig. 2013. "Fighter of government secrets endures its turn in the spotlight." *Washington Post*, October 13, 2013. https://www.highbeam.com/doc/1P2-35231487.html

E-MAIL BOMB

E-mail bombing is a type of DoS attack. The attack is carried out by sending a large amount of e-mails to the target mailbox or mailboxes. The goal of the attack is to bog down either the targeted mailboxes or the server on which they are located, denying the users of those e-mail addresses the ability to communicate with them (Houle and Pandey, 2014). E-mail bombing in the United States—and DoS attacks in general—is a crime. Under the Computer Fraud and Abuse Act, a person who intentionally sends information to another computer that impairs the ability to access data on that computer is guilty of violating that act (18 U.S. Code § 1030).

There are several reasons a person may want to e-mail bomb someone. Disrupting the victim's ability to communicate may be the goal itself. This can be done as a form of activism. In 1998, Sri Lankan embassies were e-mail bombed by a splinter group of the Liberation Tigers of Tamil Eelam, known as the Internet Black Tigers. The group made clear in the body of the e-mail that they were behind the attacks. The group's goal was to counter government propaganda (Houle and Pandey, 2014; Tribune News Services, 1998). E-mail bombing can also be done as a form of retaliation. In some instances, a person who receives junk e-mail may retaliate against the sender by e-mail bombing them (Bass et al., 1998). An e-mail bomber might attack for a mix of these two reasons. In 2017, journalists Julia Angwin, Jeff Larson, Madeleine Varner, and Lauren Kirchner wrote an article on how large tech companies enabled extremist websites to stay financed (see Angwin et al., 2017). Following publication of that article, three of the four authors of that article were e-mail bombed. Given the timing of the attack, it would seem that it was in retaliation for the article published. However, it would also seem that those launching the attack were opposed to the article's criticism of extremist websites (Angwin, 2017).

A cybercriminal can carry out e-mail bombings directly, or they can pay a service to distribute a mass amount of e-mails for them (Angwin, 2017). The attack itself can be carried out in a number of ways. Software can be set up to send large numbers of e-mails to a mailbox. This can be done from a single e-mail address, but a single point of attack can more easily be blocked once identified. Accordingly, e-mail bombing will often utilize numerous e-mail addresses. One way this is done is through a process known as list linking. With list linking, a cybercriminal will use a program to discover websites that allow you to sign up to receive e-mail from them. That program will then submit the victim's e-mail address to those websites. The victim's e-mail inbox will then be flooded with e-mail. Websites may require confirmation from the victim that they did in fact sign up to receive e-mail, but even in those instances, the victim's e-mail address will be flooded with confirmation e-mails (Angwin, 2017; Houle and Padney, 2014). Another way of using multiple points of attack is through spoofed e-mail. It is possible for cybercriminals to infect computers with malware that permits them to surreptitiously control those computers (known as bots). A network of compromised computers (known as a botnet) can then be used send massive amounts of e-mail, all from different computers.

See also: Bots and Botnets; Distributed Denial-of-Service Attack (DDoS); E-mail-related Crimes; Malware; Spam; Spoofing

Further Reading

Angwin, Julia. 2017. "How journalists fought back against crippling email bombs." *Wired*, November 9, 2017. https://www.wired.com/story/how-journalists-fought-back-against-crippling-email-bombs/

Angwin, Julia, Jeff Larson, Madeleine Varner, and Lauren Kirchner. 2017. "Despite disavowals, leading tech companies help extremist sites monetize hate." *ProPublica*, August 19, 2017. https://www.propublica.org/article/leading-tech-companies-help-extremist-sites-monetize-hate

Bass, Tim, Alfredo Freyre, David Gruber, and Glenn Watt. 1998. "E-mail bombs and countermeasures: Cyber attacks on availability and brand integrity." IEEE. https://ieeexplore-ieee-org.dist.lib.usu.edu/document/681925

Houle, Cristina, and Ruchika Pandey. 2014. "A layered approach to defending against list-linking email bombs." *IEEE*. https://ieeexplore-ieee-org.dist.lib.usu.edu/document/8376214

Tribune News Services. 1998. "U.S. tells of e-mail 'attack' by rebels." *Chicago Tribune*, May 5, 1998. https://www.chicagotribune.com/news/ct-xpm-1998-05-05-9805050148-story.html

E-MAIL-RELATED CRIMES

Billions of e-mails are sent each day from people around the world. They help facilitate business and keep people in contact with each other. At the same time, cybercriminals often use e-mails to commit crimes. Some of the crimes carried out through an e-mail include sham offers or investment schemes, e-mail bombing, cyberharassment or cyberbullying, blackmail, e-mail phishing/spoofing, fraud, and more.

Sham Offers or Investment Schemes

Many e-mails contain offers for goods or services that are enticing and seem to be bona fide proposals. It is usually offered for a sale price or with some other kind of deal or may be described as "exclusive offers" for particular individuals. These offers are often scams. Either the person "selling" the goods is a cybercriminal who wants the victim's credit card information or they take the money and never send the promised item.

E-mail Bombing

An e-mail bombing occurs when a massive number of e-mails are sent to a person or a company's server; that system is unable to handle the volume of e-mails and crashes. A cybercriminal who wants to do this only needs to compose a message in an e-mail and then send the message multiple times. If that e-mail is resent multiple times, the offender can send hundreds of e-mails quickly. When many senders use this technique, they can send hundreds of thousands of e-mails in a short time span. Hacking tools are also available for purchase online that will automate this process.

Cyberharassment or Cyberbullying

E-mails can easily be used to harass or bully another person online. The anonymity provided by the internet makes it easy for a person to send threatening or even abusive e-mails to another person. In some cases, offenders will ask others to send negative e-mails to the victims so they receive multiple harassing e-mails. These activities can be considered criminal acts, and those who are charged and found guilty face years in jail, depending on the exact circumstances.

Blackmail

Cybercriminals use e-mail to blackmail victims. They may demand money from the victim, with the threat of posting embarrassing pictures or information about the offender if the money is not paid. In some cases, the pictures are not real but have been altered by the offender. They may also threaten to harm the victim or a family member. Hackers who blackmail victims through the internet can face criminal charges with penalties of up to five years in prison and/or a monetary fine.

E-mail Spoofing/Phishing

A spoofed e-mail is one that appears to the recipient to be from a legitimate source, such as a bank, an employer, or other organization, but has actually been sent by a cybercriminal. The person who actually sent the e-mail is hidden or concealed from the recipient. The person who receives the e-mail deems the e-mail to be authentic and therefore trusts that it is safe to open. However, the e-mail may include malware (viruses, worms, or Trojans) uploaded when the recipient opens the e-mail. In some cases, the seemingly legitimate e-mail seems to be from a bank asking the victim to provide an updated user ID and password, bank account information, or credit card number. When a victim responds to the e-mail, they are giving the offender access to their banking accounts or other private information.

Appeals for Help

Also known as the "Nigerian Scam" because it often originates in Nigeria, these scam e-mails are geared to people who are willing to help another person in exchange for a promised large sum of money. Many people refer to these e-mails as the 419 e-mails, the criminal code section that controls these activities. These e-mails are often from a wealthy individual who needs help to leave the country (and once out will share his family fortune with the victim) or who needs money to travel. Some offenders are able to obtain access to a person's e-mail contacts and send an e-mail to friends and family members, claiming they have been the victim of a crime and need money to leave the country.

Fraudulent Tickets

Recipients have received e-mails that seem to be from a law enforcement agency, indicating they have been given a traffic ticket for a moving violation. The victim is asked to send their credit card information to a site, which is operated by a criminal.

Many e-mail crimes go unreported, simply because people are embarrassed that they fell for a scam, especially if they sent a large amount of money to a stranger. Some victims may feel that the offenders cannot be found, which is not always the case. If crimes are committed through e-mail, experts in digital analysis and computer forensics can often shed light on the identity of the sender. It is possible for an investigator to recover e-mails that have been deleted, along with any attachments. The IP address of a sender can often be identified. Once that information is collected, it can be analyzed and presented as evidence in a criminal trial or hearing. All e-mail crimes should be reported to law enforcement.

It is difficult to prevent these e-mails from appearing in an inbox, but people can take actions to prevent the likelihood of becoming a victim of e-mail crimes. For example, it is best to install and regularly update a spam filter that will help to identify bogus e-mails. When e-mails are received, it is a good idea to take a close look at those e-mails that look suspicious or odd. A person can look for misspellings or unusual names on the "from" line. Any e-mails that are unsolicited or contain ads that are too enticing or too good to be true should be immediately deleted.

See also: Cyberbullying; E-mail Bomb; Phishing; Spoofing

Further Reading

Bandler, John. 2017. "The cybercrime scheme that attacks email accounts and your bank accounts." *Huffington Post*, August 3, 2017. https://www.huffingtonpost.com/entry

/the-cybercrime-scheme-that-attacks-email-accounts-and_us_59834649e4b03d0624b0aca6

Federal Bureau of Investigation. 2018. *FBI releases the IC3 2017 internet crime report and calls for increased public awareness*. Washington, D.C.: FBI National Press Office, May 7, 2018. https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-ic3-2017-internet-crime-report-and-calls-for-increased-public-awareness

Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). "File a complaint." https://www.ic3.gov/complaint/default.aspx

U.S. CERT. 2008. "Computer forensics." https://www.us-cert.gov/sites/default/files/publications/forensics.pdf

ENCRYPTION

Encryption refers to the process by which data or text is encoded so that only an authorized person is able to read it. Many times, sensitive information must be sent from one office to another, or from one executive to another. That information is often e-mailed or sent electronically. If that information were to be accessed by an unauthorized person, it could result in the loss of personal data or company secrets. By encrypting the data, the sender can ensure that the material will arrive safely.

Text that people can read and understand is called plaintext, and this is the information the sender seeks to e-mail. This is also sometimes called cleartext or the input to a cipher. The plaintext is encrypted or coded by use of a mathematical algorithm. When this is done, it is called a ciphertext. Ciphertext is the encrypted plaintext, or what results when data is encrypted. The ciphertext cannot be read or understood by an individual. The ciphertext must be decrypted, or decoded, before it can be understood by a recipient. In order to change ciphertext back to plaintext, it must be decrypted by the use of a key. "Keys" are used to both encrypt and decrypt the text. To encrypt the text, a public key is used; the key is known to everyone and is distributed to the public. The recipient must have a private key to decrypt the information.

The process of encryption is often used by companies when sending data electronically so no one is able to intercept the e-mail and access or steal the data. This can include financial data, customer data, and trade secrets. Encryption also assists a person to buy something without the threat of someone stealing their credit card number.

Terrorists and other criminals use encrypted text, sometimes making it difficult for law enforcement to track their behavior. Discussions between law enforcement and companies that create algorithms have centered on the prospect of leaving an "encryption backdoor" that would allow law enforcement to decrypt messages if they can provide evidence of criminal activity. Or, similarly, those who operate social media sites to create a backdoor on their sites if there is criminal activity discovered in those platforms. The problem is simple: if those companies that design the algorithms leave a backdoor for law enforcement to decode, it would also be available to cybercriminals and hackers. They could discover this vulnerability and use it to gain access to computer systems. This is a threat to people's privacy and civil liberties, according to some.

For example, the FBI has noted that they are often unable to access cell phones that are encrypted that could provide evidence of criminal behavior. In support of their request, they noted that FBI agents were unable to access almost 8,000 devices in 2017 (although some say this figure was inflated) (Hawkins, 2018). They have asked for new laws that would require the makers of cell phones and software provide them with a way to access data if they have a warrant to do so. Those opposed to the idea explain that methods to reduce the security of encrypted data for law enforcement simply weaken encryption for all. This means that criminals would have easier access to data as well.

On the other side of the argument is those who argue that even stronger encryption is needed than what is currently used as a way to protect data and information from cybercriminals. They argue that the economy is so tied to the internet, it is essential that the safety of data be ensured. It would be devastating if it were easier for offenders to hack into information. Some experts have called for ubiquitous encryption that ensures the security of data by giving only the sender and recipient the keys to decrypt the data. This is sometimes referred to as "end-to-end" encryption.

Malware is available that allows criminals to decrypt encrypted files, allowing them to steal data that has been encrypted. This points to the need for tighter encryption. Other malware, called ransomware, encrypts a person's or company's data, making it unusable to the owner. The offender demands a sum of money to decrypt it. Many companies have been forced to pay the ransom simply to have access to their customer files. This is particularly true with health care facilities that need immediate access to files.

See also: Cryptography; Digital Signatures; Ransomware

Further Reading

Hawkins, Derek. 2018. "The Cybersecurity 202: We surveyed 100 experts. A majority rejected the FBI's push for encryption back doors." *Washington Post-Blogs*, June 11, 2018. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/06/11/the-cybersecurity-202-we-surveyed-100-experts-a-majority-rejected-the-fbi-s-push-for-encryption-back-doors/5b1d39eb1b326b6391af094a/

McConnell, Mike, Chertoff, Michael and Lynn, William. 2015. "Why the fear over ubiquitous data encryption is overblown." *Washington Post*, July 28, 2015. https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html?utm_term=.b75dabe67f59

Muncaster, Phil. 2017. "Make encryption ubiquitous, says internet society." *Infosecurity*, April 11, 2017. https://www.infosecurity-magazine.com/news/make-encryption-ubiquitous-says/

Nakashima, Ellen. 2015. "Lawmakers urge FBI to stand down on decryption push." *Washington Post*, June 1, 2015. https://www.washingtonpost.com/news/post-politics/wp/2015/06/01/lawmakers-urge-fbi-to-stand-down-on-decryption-push/

END USER LICENSE AGREEMENT

An end user license agreement (EULA) is a contract regarding a piece of software that a customer must agree to in order to use the software. Where it is a contract, a EULA will have some impact on whether certain uses of a piece of software are legal or illegal. The EULA can also have legal consequences for the developer of the software, having some impact on whether their actions in regard to the software are legal or illegal.

For customers of software, EULAs primarily impact ownership rights. Specifically, EULAs often purport to lease software to customers, not sell it to them. This limits what a customer can legally do with that software. In the United States, a software developer's ability to treat the purchase of software by a customer as a lease instead of a transfer of ownership was upheld in the federal case of *Vernor v. Autodesk*, 621 F.3d 1102 (2010). In that case, Timothy Vernor purchased copies of AutoCAD (drafting software) from a direct customer of Autodesk—the developer of the software. After purchasing the copies, Vernor then sold them on eBay. Autodesk required users of the software to agree to its license agreement in order to install the software. Among the licensing terms was the agreement that software users were unable to transfer their license to use the software to another person. Accordingly, eBay was sent a take-down notice by Autodesk with regard to Vernor's auction of AutoCAD, resulting in eBay canceling the auction. Vernor, believing he had the right to sell the software, contested Autodesk's assertions and continued to sell copies of AutoCAD on eBay. Autodesk continued to object to the sale of AutoCAD by Vernor, and Vernor ultimately filed suit to have the court declare his sale of the software to be legal. The court ultimately ruled in favor of Autodesk, holding that a software developer could treat the purchase of software by a customer as a lease if the developer specifies the transfer is in fact a lease, specifically restricts the customer's ability to transfer the software in the terms of the lease, and imposes additional use restrictions on the software.

The terms of a EULA could prohibit certain activities of a customer that would otherwise be legal if the customer owned the software in question instead of merely leasing it. As seen in the *Vernor* case above, a common restriction is a prohibition on transferring the software to someone else. Other restrictions may include a prohibition on public criticism of the software and agreeing to not uninstall parts of the program. From the standpoint of a software developer, these EULA terms make sense. Prohibiting the transfer of software does help safeguard against illegal copying of the software, while simultaneously eliminating a resale market for the software, meaning everyone who wants a copy of the software must go through the developer to get it. Curtailing criticism of software protects the developer from negative reviews that could impact the developer's ability to make a profit on the software. Software (freeware and shareware in particular) may have adware bundled with it, with the maker of the adware compensating the developer for bundling it. If a customer is able to selectively remove the adware, the profit model of the developer crumbles (Newitz, 2005).

While these restrictions make sense for software developers, they can be confusing for customers. The difference between owning software and leasing software may not be one that the average customer understands. Thus, a customer may attempt to sell a piece of software to another person, unaware that such an act is illegal. In such an instance, the customer may be found to be in violation of the developer's copyright (see Terasaki, 2014). The same could be done if a customer violates any of the other terms of the EULA. For example, a customer who alters a piece of software to make it work with their computer setup would be in violation of a EULA provision prohibiting alteration, thus running the risk of violating the developer's copyright.

Compounding the confusion for customers with EULAs is the fact that many customers never actually read the EULA for a piece of software, even though software often requires customers to signify (by checking the appropriate box) that they have read, understood, and agree to the terms of the EULA. Knowing this, several companies add farcical terms to their EULAs, aware that such terms will never be enforced. These include giving away your first-born child as a condition of using free Wi-Fi and agreeing to give your soul to a videogame retailer. At least one company went in the opposite direction, agreeing to pay $10,000 to the first person to send an e-mail address included in the middle of the EULA—a promise they followed through on (Schwartz, 2019). While such terms poke fun at EULAs, the reality is that failure to thoroughly read EULAs can, as mentioned above, result in negative legal consequences for the user of the software. The reality is that even if customers wanted to read the EULA for every piece of software and online site they use, that may be impossible. It has been estimated that for the average person in the United States, it would take approximately 76 working days to read all the EULAs and other privacy policies they agree to in the course of a year. If everyone were to actually do this, it is estimated that the productivity lost due to the time required to read those EULAs would result in a $781 billion loss annually (Madrigal, 2012; McDonald and Cranor, 2008).

A concern raised by some is the uneven bargaining position customers have in relation to software developers when it comes to EULAs (see Editorial Board, 2019; Terasaki, 2014). Generally, a customer must agree to the EULA in its entirety to use the software or service. Some of the terms customers must agree to in EULAs can be onerous. Customers may have to agree to monitoring by the developer, waiving claims against the developer if the software ruins their computer, and to be bound by any changes in the EULA—which the developer may be able to make without notice to the customer (Newitz, 2005). It is possible that if a EULA is too one-sided in favor of a software developer, a court may deem the EULA unconscionable and thus legally unenforceable, in whole or in part (Terasaki, 2014). This happened in the case of *Bragg v. Linden Research, Inc.*, 487 F. Supp. 2d 593 (2007). In that case, Marc Bragg was a user of software created by Linden Research called Second Life—a virtual world on the internet. Bragg had to agree to a EULA to use Second Life. Bragg purchased several parcels of land in Second Life and acquired other items in the virtual world as well. Following a purchase made by Bragg that Linden Research claimed was outside the permitted channels, Linden Research froze Bragg's account, depriving him access to the parcels of land he purchased and the other items he had acquired. It claimed it was permitted to do so under the terms of the EULA. Bragg filed suit against Linden Research in court, and Linden Research filed a motion to have the case resolved via arbitration as per the terms of the EULA. In finding the arbitration clause of the EULA unconscionable and thus unenforceable, the court noted several provision in it that were clearly in favor of Linden Research. Among those were a provision requiring that users seeking to resolve a dispute do so through arbitration at Linden Research's place of business (while Linden Research itself could choose to freeze a user's account in its sole discretion) and a provision requiring the arbitration proceeding to be confidential (Terasaki, 2014).

There are additional legal issues software developers must be aware of when drafting a EULA beyond drafting it in a way that will not be unconscionable. Software developers that do not properly disclose what their software does can end up in legal trouble. This happened to Sony BMG in 2005. Sony BMG downloaded software onto the computers of customers who purchased select CDs from them. The software included a form of DRM software—software intended to prohibit unauthorized copying of intellectual property, such as songs on a CD. The EULA provided by Sony BMG did not mention the DRM component of the software or that fact that it would be downloaded onto a customer's computer (Russinovich, 2005). Additionally, the software sent information about user's music listening habits to Sony BMG, despite the fact that the EULA specifically noted that personal information would not be collected (Electronic Frontier Foundation, 2019). This lack of disclosure in the EULA of the properties of the software made it appear to be spyware—software that is installed on a computer without the user's knowledge and that transmits information to another party. Sony BGM ultimately faced several lawsuits over this software. This included a U.S. class-action suit that Sony BMG settled (Associated Press, 2005) and lawsuits from 42 individual states that Sony BMG also settled for a total of over $5 million (McMillan, 2006).

See also: Copyright Infringement; Digital Millennium Copyright Act; Digital Rights Management; Open-Source; Spyware

Further Reading

Associated Press. 2005. "Sony BMG tentatively settles suits on spyware." *New York Times*, December 30, 2005. https://www.nytimes.com/2005/12/30/technology/sony-bmg-tentatively-settles-suits-on-spyware.html.

Editorial Board. 2019. "How Silicon Valley puts the 'con' in consent." *New York Times*, February 2, 2019. https://www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html

Electronic Frontier Foundation. 2019. "Sony BMG litigation info." Electronic Frontier Foundation. https://www.eff.org/cases/sony-bmg-litigation-info

Madrigal, Alexis C. 2012. "Reading the privacy policies you encounter in a year would take 76 work days." *The Atlantic*, March 1, 2012. https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/

McDonald, Aleecia M., and Lorrie Faith Cranor. 2008. "The cost of reading privacy policies." *I/S: A Journal of Law and Policy for the Information Society* 4, 3: 543–568.

McMillan, Robert. 2006. "Sony rootkit settlement reaches $5.75M." *PCWorld*, December 22, 2006. https://www.pcworld.com/article/128310/article.html.

Newitz, Annalee. 2005. "Dangerous terms: A user's guide to EULAs." *Electronic Frontier Foundation*. https://www.eff.org/wp/dangerous-terms-users-guide-eulas

Russinovich, Mark. 2005. "Sony, rootkits and digital rights management gone too far." *TechNet* (blog), October 31, 2005. https://blogs.technet.microsoft.com/markrussinovich/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far/

Schwartz, Matthew S. 2019. "When not reading the fine print can cost your soul." National Public Radio, March 8, 2019. https://www.npr.org/2019/03/08/701417140/when-not-reading-the-fine-print-can-cost-your-soul

Terasaki, Michael. 2014. "Do end user license agreements bind normal people?" *Western State University Law Review* 41, 2: 467–489.

ENGRESSIA, JOSEF CARL, JR. (1949–2007)

Josef Carl Engressia Jr., otherwise known as Joybubbles, was a key person in the 1970s "phone phreaking" subculture, whose members found ways to hack into telephones. After being arrested in 1971, Engressia eventually worked Mountain Bell in Denver, Colorado, to help them solve security weaknesses in their network and prevent others from taking advantage of the vulnerabilities.

Engressia was born in 1949 in Richmond, Virginia, but his family moved often. Born blind and with an IQ of 172, Engressia became interested in telephones at an early age. When he was seven years old, Engressia realized he could activate phone switches by whistling a certain frequency. When he whistled a tone at 2,600 Hz into a phone receiver, he could dial anywhere for free. Because of this skill, Engressia was given the nickname "The Whistler."

Because of his obsession with the phone, Engressia's parents refused to have a phone in the home. Engressia chose to attend the University of South Florida, where he studied math. While in college, he could call long-distance for free by whistling the right tones, as he had learned when he was younger. Engressia began to charge other students one dollar to place a free long-distance call, and it wasn't long until someone reported him. Engressia was suspended from school in 1968 and fined $25 but was reinstated quickly, and he eventually graduated from the university with a degree in philosophy.

This incident became public through the media, and the general public quickly became aware of weaknesses of the phone system. One article that described the activities and culture of the phone phreakers and brought a great deal of attention to their activities was written by Ron Rosenbaum, entitled "Secrets of the Little Blue Box." In the article, published in *Esquire* magazine, Rosenbaum wrote about Engressia and other phone phreakers who had successfully hacked the phones and had created a "blue box" that could be used to override the phone system and cheat the company to make calls around the world without cost and without being traced.

After graduation, Engressia moved to Tennessee and continued to make free phone calls by whistling the right tone. One day, as he was making a call, he "dialed" a wrong number and spoke with an operator for Bell Telephone in

Montreal. The operator became suspicious and started to monitor Engressia's phone calls, even though it was illegal. Engressia had discovered a way to call around the world to himself by calling on one phone and answering another, all for free. The employee eventually called the police and described what Engressia was doing. The police raided Engressia's home. He was arrested in 1971 and pleaded not guilty to theft of service, but the judge reduced the charges to malicious mischief. Engressia was given a suspended sentence on the condition that he never work with phones again.

As phone companies moved to digital systems, Engressia could no longer make free calls by whistling. Engressia moved to Minnesota in 1982 and helped with research concerning how to control the odor of hog waste (because of his keen sense of smell). He became an ordained minister for the Church of the Eternal Childhood, a church he established. In 1991, he declared that he was legally changing his name to Joybubbles and that he was "the age of five forever." He often acted very childlike, which some attributed to the fact that he was sexually abused as a child by a teacher at a school for blind children. He decided to use the phone to record his life story on a show called "Stories and Stuff," a series of audio files in which he discussed his thoughts on different issues.

Engressia died of a heart attack in 2007 at the age of 58.

See also: Hacker and Hacking

Further Reading

BBC. 2017. "A Call from Joybubbles." March 13, 2017. http://www.bbc.co.uk/programmes/b08hlnjq

Martin, Douglas. 2007. "Joybubbles, 58, Peter Pan of hackers, dies." *New York Times*, August 20, 2007. https://www.nytimes.com/2007/08/20/us/20engressia.html?mtrref=www.bing.com&gwh=BFD9FC9689/0CD1B6746BBC5A2888D609&gwt=pay

Otte, Jef. 2011. "Remembering Joybubbles: Short-term Denver resident, general weirdo and hacker O.G." *Westword*, August 8, 2011. https://www.westword.com/arts/remembering-joybubbles-short-term-denver-resident-general-weirdo-and-hacker-og-5814712

Rosenbaum, Ron. 1971. "Secrets of the little blue box." *Esquire* (October): 117–226.

Whistle Productions. 2016. *Joybubbles*, Documentary Film. http://www.joybubblesthemovie.com/

ENTERTAINMENT, EFFECTS ON

Cybercrime can affect the entertainment industry, in particular with regard to intellectual property theft. The financial impact it has on the industry is substantial. It is estimated that between $225 billion and $600 billion worth of U.S. intellectual property is stolen annually (Commission on the Theft of American Intellectual Property, 2017). Intellectual property theft includes crimes that would not be considered cybercrimes, and crimes that would not impact the entertainment industry. For example, the trafficking of counterfeit goods (knock-off purses, watches, etc.) is considered intellectual property theft. Such a crime does not require cyber means to commit, nor does it impact the entertainment industry. When looking at the impact of intellectual property theft on the entertainment industry, the thefts of concern would be illegal downloads of movies, songs, video games, and similar intangible items. Looking at those types of intellectual property theft alone, the annual loss is in excess of $200 billion (Business Action to Stop Counterfeiting and Piracy and International Trademark Association, 2016). Intellectual property theft is a fairly widespread problem. Unlike other cybercrimes, intellectual property theft is committed by a large portion of the population. A survey conducted in the United Kingdom found that 60 percent of people admitted to they had either illegally downloaded or illegally streamed intellectual property (Music Business Worldwide, 2018).

These losses to the entertainment industry can have a compounding economic effect. Entertainment businesses lose revenue when someone illegally downloads intellectual property Lowered revenue can lessen the amount of intellectual property an entertainment business is able to produce in the future. This, in turn, lessens the number of employment opportunities offered by that entertainment business (Siwek, 2007). Losses by an entertainment business can have an effect on law-abiding consumers as well. To compensate for losses suffered, an entertainment business may increase the amount a company charges for its intellectual property. The mere threat of intellectual property theft can have this same effect, as entertainment businesses often pay to have measures in place to prevent the theft of their intellectual property.

Different methods have been employed to try to remedy intellectual property theft. The availability of streaming services—services where customers pay a monthly fee to have access to a large library of creative works—is sometimes thought to have reduced intellectual property theft by making works widely available. However, the availability of these services has not stopped the increase in incidents of intellectual property theft (Music Business Worldwide, 2018). In fact, those services also appear to suffer losses on account of intellectual property theft. One estimate shows that streaming services like Netflix, Amazon, and Hulu will lose over $50 billion between 2016 and 2022 due to intellectual property theft (Clarke, 2017).

Another method used to curtail intellectual property theft is the employment of DRM. DRM is the process of encoding digital intellectual property in a manner designed to prevent the unauthorized distribution of that intellectual property. Circumvention of DRM is proscribed in the United States under the Digital Millennium Copyright Act. Although the use of DRM may help prevent intellectual property theft, whether it ultimately helps the bottom line of an entertainment business is a different matter. Research indicates that an entertainment business could see increased profits by not using DRM (Zhang, 2014). Some artists—such as video game developer Tommy Refenes and author Charlie Stross—have expressed sentiments in line with this finding, indicating that the use of DRM can alienate dedicated paying customers, which can decrease sales in the long run (Stross, 2012; Thier, 2013).

In addition to concerns of the economic viability of using restrictive measures to prevent intellectual property theft, there is some indication that use of less restrictive methods may result in a decrease of intellectual property theft. One study found that among people who admitted to illegally downloading and streaming intellectual property, 83 percent attempted to access those creative works by legal means before resorting to illegal means to access them (Music Business Worldwide, 2018).

The impact of cybercrime on entertainment is not just economic. It can also affect the quality and enjoyment of the entertainment as well. This is particularly the case where performances are recorded by fans. With the prevalence of cell phones, this occurs quite frequently. Using phones to record performances can be distracting to other patrons, but perhaps the bigger concern is the fact that it is generally considered intellectual property theft. The artist—whether a musician, comedian, or writer of a musical—generally owns the rights to the material being performed, and unauthorized distribution of that performance would violate their copyright. From a practical standpoint, it can also negatively impact an artist's ability to refine their work. The Lumineers—a folk rock band—used one of their tours to perform new songs for their fans and work on improving the songs along the way (Stilwell and Cox, 2017). Comedians often do similar with new routines. Comedian Chris Rock indicated that this is how comedy routines are refined—trying out new bits with audiences, learning what works and what does not, and refining the act accordingly (Izadi, 2014). Rock indicated that with the prevalence of cell phones at shows, comedy bits get released before they are fully refined, leading to a performance that may not be the final product yet. Rock believes this can lead comedians to be cautious in the material they prepare for fear that their not-yet-vetted acts might get recorded, distributed online, and be criticized before all the kinks are worked out (Izadi, 2014).

A separate issue arises when recorded performances spoil the experience of viewing the performance for other fans. In early 2019, a recording of *Avengers: Endgame*—a highly anticipated super hero film—was posted online. It appears the recording was made during an early screening of the film. For those law-abiding fans who wanted the excitement of viewing the film in theaters without knowing beforehand what was going to happen, a recording like this can be frustrating. Such fans can avoid watching the recording, but it may become difficult to avoid unintentional mentions of plot points online. The directors of *Avengers: Endgame* encouraged fans to avoid spreading such information so as not to spoil it for those fans (Spangler, 2019).

See also: Copyright Infringement; Digital Millennium Copyright Act; Digital Rights Management; Economy, Effects on

Further Reading

Business Action to Stop Counterfeiting and Piracy and International Trademark Association. 2016. "The economic impacts of counterfeiting and piracy." https://cdn.iccwbo.org/content/uploads/sites/3/2017/02/ICC-BASCAP-Frontier-report-2016.pdf

Clarke, Stewart. 2017. "Piracy set to cost streaming players more than $50 billion, study says." *Variety*, October 30, 2017. https://variety.com/2017/tv/news/piracy-cost-streaming-players-over-50-billion-1202602184/

Commission on the Theft of American Intellectual Property. 2017. "Update to the IP Commission Report." http://ipcommission.org/report/IP_Commission_Report_ Update _2017.pdf

Izadi, Elahe. 2014. "Chris Rock isn't the only comedian who thinks cellphones are killing stand-up comedy." *Washington Post*, December 2, 2014. https://www.washingtonpost .com/news/arts-and-entertainment/wp/2014/12/02/chris-rock-isnt-the-only -comedian-who-thinks-cell-phones-are-killing-stand-up-comedy/?utm_term= .d553fdc506fd

Music Business Worldwide. 2018. "83% of people who pirate music, film and TV tried to find it legally first, says survey." Music Business Worldwide, June 6, 2018. https://www .musicbusinessworldwide.com/83-of-people-who-pirate-music-film-and-tv-tried-to -find-it-legally-first-says-survey/

Siwek, Stephen E. 2007. "Reducing government consumption, increasing personal wealth." Institute for Policy Innovation. https://www.riaa.com/wp-content/uploads/2015/09 /20120515_SoundRecordingPiracy.pdf

Spangler, Todd. 2019. "Marvel 'Avengers: Endgame' footage reportedly leaks online." *Variety*, April 16, 2019. https://variety.com/2019/digital/news/marvel-avengers-endgame -footage-leaks-online-1203190583/

Stilwell, Rachel, and Makenna Cox. 2017. "Phone recordings of concerts are more than just annoying, they're potentially illegal: Guest post." *Billboard*, March 17, 2017. https:// www.billboard.com/articles/business/7724330/phone-recordings-concerts-illegal -federal-bootlegging-laws

Stross, Charlie. 2012. "The case against DRM on eBooks." *Gizmodo*, April 25, 2012. https:// gizmodo.com/the-case-against-drm-on-ebooks-5905023.

Thier, Dave. 2013. "DRM hurts companies more than piracy, developer argues." *Forbes*, March 19, 2013. https://www.forbes.com/sites/davidthier/2013/03/19/drm-hurts -companies-more-than-piracy-developer-argues/#372de7716aa6

Zhang, Laurina. 2014. "Intellectual property strategy and the long tail: Evidence from the recorded music industry." Researchgate. https://www.researchgate.net/publication /275639877_Intellectual_Property_Strategy_and_the_Long_Tail_Evidence_from_the _Recorded_Music_Industry

EQUIFAX BREACH

In September 2017, Equifax, a company that monitors and reports on the credit of millions of people was hacked, exposing the personal information of millions of people. The company announced that the names, birthdays, addresses, driver's licenses, and social security information was stolen for an estimated 143 million Americans—about half the country's population. Data was also stolen from residents of Canada and the United Kingdom. This breach would make it easy for criminals to steal the identities of the victims. Many cybercrime experts claimed that the breach was one of the largest and most extensive hacks to date. The company announced that it was working with a cybersecurity firm and with the Federal Trade Commission (FTC) to investigate the breach.

The breach was made worse because the hackers allegedly accessed the files between mid-May and July 2017, but the company did not make that information public until six weeks after it happened. Moreover, it was reported that three top officials in the company sold their shares—almost $2 million in shares—days after the breach was discovered but long before reporting the breach to the public. Many accused these officials of insider trading.

The breach was reportedly the result of a vulnerability in Apache Struts, a free, open-source software. There were many vulnerabilities in the software, and patches were available to solve the problems. Because the patches have been available for some time for many of the vulnerabilities, it was thought that Equifax should have had them in place.

In light of the breach, Equifax offered victims a free year of credit-report monitoring services. But security experts suggested that free credit monitoring would not prevent a criminal from stealing a person's identity, and recommended instead that consumers put a "freeze" on their accounts to prevent thieves from having access to account information. It was also suggested that people watch their credit reports and monitor bank accounts and report any suspicious activity. So the company then opted to waive all fees or repay fees for those who sought to put a freeze on their credit as a way to prevent hackers from stealing their assets.

Not long after the breach was announced, members of the U.S. Senate Finance Committee began asking questions about the loss of customers' personal data. A few days after the hearings, 36 Senators asked federal officials from the Department of Justice, the Security and Exchange Commission (SEC), and the FTC to look into the actions of Equifax officials.

In the end, it was reported that there were a series of deficiencies that resulted in the hacking, including poor security safeguards and limited protection measures to protect those affected. It was also discovered that Equifax retained personal information too long. Executives at the company have announced that it has undertaken efforts to improve its security and policies for destroying data.

Breaches are becoming more common and affect more people, largely because there is more information collected and stored digitally than ever before. Unfortunately, sensitive data such as social security numbers are often not protected sufficiently.

See also: Hacker and Hacking; Vulnerability

Further Reading

Bogost, Ian. 2017. "The banality of the Equifax breach." *The Atlantic*, September 8, 2017. https://www.theatlantic.com/technology/archive/2017/09/the-equifax-breach-marks-the-end-of-shame-over-data-security/539202/

Goldstein, Matthew. 2017. "Senators seek answers on Equifax breach, including details on stock sales." *New York Times*, September 11, 2017. https://www.nytimes.com/2017/09/11/business/equifax-greach-stock-sale.html?mcubz=0

Gressin, Seena. 2017. "The Equifax data breach: What to do." Federal Trade Commission, Consumer Information, September 8, 2017. https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

Liedtke, Michael. 2017. "Hackers steal data from Equifax files." *Akron Beacon Journal*, September 8, 2017.

NBC News. 2017. "Here's what you can do about that Equifax data breach." NBC News, September 11, 2017. https://www.nbcnew.com/tech/security/here-s-what-you-can-do-about-equifax-data-breach-n800501

Popken, Ben. 2017. "The one move to make after Equifax breach." NBC News, September 12, 2017. https://www.nbcnews.com/business/consumer/one-move-make-after-equifax-breach-n800776

Schroeder, Pete. 2017. "US senator on Equifax hack: 'Somebody needs to go to jail.'" *U.S. News and World Report*, September 13, 2017. https://www.usnews.com/news/top-news/articles/2017-09-12/us-senator-on-equifax-hack-somebody-needs-to-go-to-jail.

Weise, Elizabeth. 2017. "How did the Equifax breach happen? Here are some answers and some questions." *USA Today*, September 12, 2017. https://www.usatoday.com/story/tech/2017/09/12/how-did-equifax-breach-happen-here-some-answers-and-some-questions/658343001/

ETHICS

Ethics refers to the set of beliefs and practices a person adheres to when making decisions in life. Just because an act is criminal does not necessarily mean it is also considered unethical, such as sit-ins during the Civil Rights Movement. People who consciously violate laws in accordance with their belief system act according to an ethical code. Cybercriminals may have an ethical code they adhere to when committing cybercrime. This, of course, does not mean that every cybercriminal's misdeeds stem from an ethical code. Criminal actions committed simply because the criminal wants to commit crime would not generally be considered ethical. Those crimes that are committed in accordance with a set of beliefs would be considered ethical. There are many specific groups of cybercriminals that do adhere to such a code, and it is important to know what those codes are when trying to understand or apprehend cybercriminals.

For some cybercriminals, there may be a specific crime they do not believe should be criminal, and they use cyber methods to violate that law while avoiding detection by law enforcement. An example of this would be drug use and drug trafficking. There are a number of people who are opposed to the criminalization of drugs and believe that use of drugs should not be a crime. There are sites that are or have been on the internet that permit the buying and selling of drugs. Silk Road is perhaps the most notable of these sites. Silk Road operated on the deep web and allowed users to conduct anonymous drug transactions using Bitcoin. While such actions violate the law in many locations, those buying and selling drugs on such a site may view their actions as ethical because they view the criminalization of drugs as unethical (Bearman et al., 2015).

Another example would be intellectual property theft. Many people do not believe that the current system of copyright law is fair. For example, some may disagree with the use of digital rights management, or believe that abandonware should be free to download without legal repercussion. Such a person may simply download abandonware anyway, or take efforts to circumvent digital rights management, even though these acts may be deemed illegal. Again, a person doing this may view such actions as ethical because they are in accordance with how they believe the law should be, even though it may be in violation of the law.

Some cybercriminals do not violate a specific law because they do not agree with that law. Rather, there is some sort of wrong they wish to prevent, and they believe that using criminal means to prevent that wrong is proper, and thus ethical. Hacktivists are an excellent example of this. One instance of this would be the hack of Sony Pictures by North Korea. The hack appears to have been precipitated by Sony's production of *The Interview* (2014)—a movie whose plotline involved the assassination of North Korean president Kim Jong-un (1983–). For those hackers, they viewed the release of The Interview as wrong, and hacking was a way to prevent that wrong (Peterson, 2014). Thus, they viewed the use of hacking to prevent that wrong as ethical.

Another example is the hack of the Ashley Madison website in 2015. Ashley Madison was a site where individuals seeking to have an extramarital affair could meet and arrange such affair. Hackers accessed the account data of site users and released that data to the public. The hacker group saw the affair website as patently dishonest, and thus unethical. The dishonesty they were combating was not the affairs taking place, per se, but rather the company's practice of never deleting personal information of clientele. This attack was seen as a way to combat the dishonesty of the company and was thus ethical in their eyes (Thomsen, 2015).

Another group of cybercriminals may have a specific ideal they view as important, and attempts to secure that ideal—be those attempt criminal or legal—would be viewed as ethical. Perhaps most prominent among these are the twin ideals of privacy and transparency. There are groups, such as cypherpunks, who place great value on privacy and take actions to achieve it (Hughes, 1993). Some of those actions may be illegal, but if it advances the cause of increased privacy, those cypherpunks would view those actions as ethical.

There are those who advocate individual privacy and organizational or government transparency. For example, Edward Snowden (1983–) leaked numerous classified CIA documents to the world, revealing the extent to which the U.S. government was collecting data on citizens. Snowden believed this was a massive breach of individual privacy. Conversely, he believed the government should have been transparent with such matters (Hill, 2013). WikiLeaks falls into the same category. It promotes transparency in government, business, and other organizations, but zealously protects the anonymity of its whistleblowers. Again, many of the acts taken to assure these objectives are criminal. Nonetheless, those perpetrating the acts—such as Snowden or Julian Assange of WikiLeaks—are treated as heroes by many who likely share the same ethical code regarding privacy and transparency (Cassidy, 2013; Watkins, 2016).

See also: Anonymous; Ashley Madison Breach; Hacker and Hacking; Hacktivism; Motives; WikiLeaks

Further Reading

Bearman, Joshuah, Joshua Davis, and Steven Leckart. 2015. "The rise & fall of Silk Road, part 1." *Wired*, No. 23.5.

Cassidy, John. 2013. "Why Edward Snowden is a hero." *The New Yorker*, June 10, 2013. https://www.newyorker.com/news/john-cassidy/why-edward-snowden-is-a-hero

Hill, Kashmir. 2013. "Why NSA IT guy Edward Snowden leaked top secret documents." *Forbes*, June 10, 2013. https://www.forbes.com/sites/kashmirhill/2013/06/10/why-nsa-it-guy-edward-snowden-leaked-top-secret-documents/#1e7a56de5673

Hughes, Eric. 1993. "A cypherpunk's manifesto." https://www.activism.net/cypherpunk/manifesto.html

Peterson, Andrea. 2014. "The Sony Pictures hack, explained." *The Washington Post*, December 18, 2014. https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.9ba3501ced1f

Thomsen, Simon. 2015. "Extramarital affair website Ashley Madison has been hacked and attackers are threatening to leak data online." *Business Insider Australia*, July 20, 2015. https://www.businessinsider.com/cheating-affair-website-ashley-madison-hacked-user-data-leaked-2015-7

Watkins, Eli. 2016. "Jill Stein: 'No question' Julian Assange is a hero." *CNN*, August 6, 2016. https://www.cnn.com/2016/08/06/politics/jill-stein-julian-assange-green-party-convention/index.html

EUROPEAN CYBERCRIME CENTER

Similar to events and trends in the United States, cybercrime has become a serious matter for European countries. Some estimates show that cybercrime costs European Union (EU) member states about €265 billion each year. As a way to combat this trend, Europol (the law enforcement agency for the EU) established the European Cybercrime Center (EC3) in 2013. The intent behind the new organization was to strengthen law enforcement's response to cybercrime so that there was a more efficient and more effective approach to handling cybercrime events. The new agency was given the mission of assisting law enforcement authorities in the European Union to deter cybercrime and investigate events when they occurred.

The primary task of the newly created EC3 was to disrupt and prevent the cybercrime activities of global organized crime networks that are responsible for many of the cybercrimes committed that cause serious harm to victims. This is essential as these offenses have the potential to injure the critical infrastructure in any of the countries, as well as their information systems. To fulfill these goals, the membership of the EC3 includes two forensics teams—one focuses on digital forensics while the other emphasizes documents. There are two strategy teams, one for outreach and one for support. A cyberintelligence team is in charge of collecting information about cybercrimes to identify potential threats, but also to keep data on trends and patterns for events. In addition to these specialized groups, the Joint Cybercrime Action Taskforce (J-CAT) was also established to investigate critical international cybercrime events that have an impact on EU member states. Together, these groups seek to create workable partnerships among all of the members and then develop a plan for the prevention of cybercrimes, while at the same time increasing the public's awareness of online crimes.

The agents working in EC3 rely on existing law enforcement techniques and activities when investigating offenses. The crime areas they focus on include cybercrime, high-tech crimes, social engineering, child sexual exploitation, forgery of money and means of payment, payment fraud, and money laundering.

EC3 participates in any operations or investigations that are requested by member states. The new agency also serves as the clearinghouse for information and issue analyses of events when they occur. The organization also provides expertise to agencies that request it, as well as training in cybercrime investigations.

Members of EC3 often work cooperatively with other law enforcement agencies, such as the FBI and the U.S. Department of Justice. As a result of one cooperative investigation in 2014, law enforcement agents closed dozens of illegal websites and took the operators into custody. According to officials at EC3, agents were able to identify users of Tor, a network that encrypts the identities of users and their activities online. The websites they closed provided a market for illegal drugs and weapons. One of the men arrested was Blake Benthall, from California, who oversaw the operation of Silk Road 2.0, a website popular for selling illegal goods. Also arrested at that time was Thomas White, another operator of Silk Road 2. Others arrested were from Sweden, Hungary, Ireland, Spain, and the United Kingdom.

In 2016, EC3 warned that acts of cybercrime are on the rise and that the number of cybercriminals is increasing. Moreover, there are many more opportunities to commit acts of cybercrime online. To combat this, personnel at EC3 took part in 131 investigations in 2015, which was an increase from 72 in 2014. However, they noted that cybercriminals are constantly developing new methods to carry out attacks, which are then sold or provided to criminals around the world, including state actors and terrorists. They also noted the increased use of encryption by offenders to hide their activities.

See also: Encryption; Federal Bureau of Investigation; Silk Road

Further Reading

Barnes, Julian E. 2016. “Europol warns of cybercrime surge: Cybercrime Centre supported 131 successful operations last year, nearly double 2014’s number.” *Wall Street Journal*, September 28, 2016. https://www.wsj.com/articles/europol-warns-of-cybercrime-surge-1475042402

Dalton, Matthew and Andres Grossman. 2014. “Arrests signal breach in ‘Darknet’ sites: Police find website operators that used encrypted Tor network to traffic in illegal drugs, guns.” *Wall Street Journal*, November 7, 2014. https://www.wsj.com/articles/illegal-websites-seized-by-eu-u-s-authorities-1415368411

Europol: EC3. https://www.europol.eruopa.eu/about/eruopol/european-cybercrime-centre-ec3

Robinson, Neil, Emma Disley, Dimitris Potoglou, Anais Reding, Deirdre May Culley, Marvse Penny, Maarten Botterman, Gwendolyn Carpenter, Colin Blackman, and Jeremy Millard. 2012. *Feasibility study for a European Cybercrime Centre*. Santa Monica, CA: Rand Corporation. https://www.rand.org/pubs/technical_reports/TR1218.html

EXPLOIT KIT

An exploit kit is a hacking toolkit or “crimeware” that is used by cybercriminals to upload malware onto other computers, thus giving them access to or control over another person’s computer. The kits are often software programs that collect information on other computers and are able to identify potential weak spots, called backdoors or vulnerabilities, in other machines. Once that has been found, the exploit then uploads malware onto the vulnerable machine. Most of the time, the computer owner is not aware that the malware has been uploaded onto their machine. The malware can be a virus, botnet, ransomware, or a variety of other types of malware. The malware is downloaded in a "drive-by attack," which refers to a download that occurs without the owner's knowledge. Most of the time the downloaded software is a form of malware.

The exploit kits are usually very simple to use and allow criminals with little technical knowledge to carry out attacks on a variety of sites in an attempt to steal corporate data and/or personal information from others. The kits are created by programmers but are available for sale or rent to a third party on the dark web. Many of the kits originate in Russia or China. Most kits are updated regularly by the creator to add new exploits so it will target new vulnerabilities on different networks. The price of the exploit kit will depend on the quality of the program, its age, the malware involved, or the length of time the malware will be used. The programs allow anyone to become a "hacker for profit." Cybercrimes using exploit kits most often target victims in the United States.

If a person purchases an exploit kit, they will be able to use them for a variety of offenses. For example, they can create botnets and then send out thousands of spam e-mails in order to crash a website through a DoS attack. This may be done by a competitor or by a disgruntled employee or customer who seeks to harm a company or organization. An exploit kit will also allow an offender to carry out financial crime by sending out a fake e-mail that seems legitimate, tricking a victim into providing personal information (passwords, bank accounts, or credit card numbers) to an offender. There are an unlimited number of offenses that can be carried out.

The first exploit kit identified, the WebAttacker kit, was made available in 2006. It was sold for $20 and was discovered in the Russian underground market. The exploit was distributed through spam and compromised websites. Another exploit kit found in 2006 was Mpack, which was created by three Russian programmers. This program was more complex and cost an offender $1,000 to purchase.

Since that time, there have been numerous exploit kits developed and available for sale. For example, the NeoSploit exploit kit, developed in 2007, was available from a Russian site and quickly developed a reputation as being a reliable and advanced exploit kit. It was used often by cyberoffenders because it could be modified to suit their needs. Another benefit was that the authors continued to add new exploits for vulnerabilities, keeping it updated.

An exploit kit called Nuclear Pack appeared in 2009. This became one of the most widely used kits because it could install many types of malware. Another popular kit, called Blackhole, also became popular when it was developed in 2010. This kit, also available from the Russian underground market, allowed offenders to steal banking credentials, leading to the theft of millions of dollars over the span of a few years. The 27-year-old, unidentified Russian and creator of Blackhole, was identified as "Paunch." He reportedly earned up to $50,000 each month by selling the malware kit. The kit cost between $500 and $700 to rent, but for an additional $50 a month, the kit could be personalized. Along with the malware, customers could also rent a "crypting" service that would hide the malware and make it harder to detect. Paunch was eventually caught, convicted, and sentenced to a seven-year prison term in a Russian prison.

A similar kit, Whitehole, was discovered in 2013. This kit cost a buyer up to $2,000. It was known for being able to evade detection and for its ability to load up to 20 malicious files at a time. In the following year, a kit named Magnitude received attention after cybercriminals used it in an attack on Yahoo. In 2015, the Angler exploit kit was popular among cyberthieves, attacking news, entertainment, and political sites. Angler could be used easily by people who had little or no technical knowledge, making it well-liked. A more recent exploit was named Icepack and is available on the internet for around $400.

It is important that computer owners and businesses take action to prevent attacks from an exploit kit. Users should be careful when visiting websites and look for clues that they are not genuine sites. Users should install antivirus programs and keep them updated. Finally, security patches should be installed if they are issued by the program's vendor.

See also: Dark Web; Malware; Vulnerability; Zero-Day Attacks

Further Reading

Chen, Joseph C. and Brooks Li. 2015. "Evolution of exploit kits." TrendMicro. https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits.pdf

Howard, Fraser. 2015. "A closer look at the Angler exploit kit." Sophos News, July 21, 2015. https://news.sophos.com/en-us/2015/07/21/a-closer-look-at-the-angler-exploit-kit/

Messmer, Ellen. 2011. "MPack, NewSploit and Zeus top most notorious web attack toolkit list." *Network World*, January 18, 2011. https://www.networkworld.com/article/2198847/malware-cybercrime/mpack--neosploit-and-zeus-top-most-notorious-web-attack-toolkit-list.html

Segura, Jerome. 2018. "Exploit kits: Winter 2018 review." Malwarebytes, March 29, 2018. https://blog.malwarebytes.com/threat-analysis/2018/03/exploit-kits-winter-2018-review/

Simmonds, Mike. 2016. "Beware the drive-by attack." Information Security Buzz, September 13, 2016. https://www.informationsecuritybuzz.com/articles/beware-drive-attack/

Zaharia, Andra. 2016. "The ultimate guide to Angler Exploit Kit for non-technical people (Updated)." Heimdal Security, May 18, 2016. http://heimdalsecurity.com/blog/ultimate-gide-angler-exploit-kit-non-technical-people/

F

FEDERAL BUREAU OF INVESTIGATION

The FBI is a law enforcement agency in the United States that operates at the national level under the Department of Justice. The FBI investigates numerous crimes, from white-collar crime to terrorism. Among federal agencies, the FBI is at the forefront of investigating cybercrime.

The FBI first appears to be involved in the investigation of cybercrime in the early 1990's. In 1994, the FBI launched Operation Innocent Images—an investigation into the world of child pornography and child sexual exploitation on the internet. The initial investigation that led to the operation was not cyber-related at all. It started with a missing child investigation in Maryland in 1993. While canvasing the missing child's neighborhood, law enforcement encountered two men who were becoming friendly with local children by giving them things and taking them places. Law enforcement discovered that these men had been sexually abusing children for decades and that they had moved online to try and lure in more child victims. The men were convicted of child abuse. They were not charged in conjunction with the missing child as there was no evidence to tie them to that case. The child was never found. The FBI used the information they gathered from this investigation—namely the fact that child predators were using the internet to lure victims—to launch Operation Innocent Images. As part of this operation, agents pretended to be children online to draw out pedophiles. This same work is carried out by the FBI today under its Violent Crimes Against Children Unit (Federal Bureau of Investigations, 2018b).

In 1994, the FBI was also involved in the investigation of what is believed to be the first incident of online bank theft. In that case, hackers infiltrated the computers of the bank and transferred money out of customer accounts into accounts set up by the hackers to receive the money. The amount stolen was over $10 million. The FBI were able to initially arrest a Russian couple involved in the scheme, and that couple assisted with their investigation. In the end, the FBI worked with Russian authorities and ultimately arrested Vladimir Levin, the mastermind of the scheme (Federal Bureau of Investigation, 2018b).

The FBI has at times been tasked with cybercrime-related duties in addition to the investigation of cybercrimes. The National Infrastructure Protection Center (NIPC) was established as part of the FBI in 1998. Its purpose was to track emerging computer threats and coordinate responses to those threats for the government. Despite the increased attention that cybercrimes seemed to be getting at this point, the FBI appeared to be unable to fully staff all the cybercrime-specific positions it had hoped to. In 1999, the FBI's goal was to have 243 agents assigned to cybercrimes, but only a few officers were assigned to cybercrimes at just 10 of the FBI's field offices. At this same time, the number of officers assigned to the NIPC was declining—just a year after it was established (Suro, 1999). The NIPC was moved from the FBI to the Department of Homeland Security in 2002.

As part of its efforts to apprehend cyber criminals, the FBI helped establish the Internet Fraud Complaint Center (now known as the Internet Crime Complaint Center) in 2000. The Center's website allows victims of cybercrime to submit that information to the FBI for investigation. There have been over four million complaints reported to the Center since its founding. Currently, the Center receives about 284,000 complaints annually (Federal Bureau of Investigation, 2018c). These complaints have led to the arrest and conviction of cybercriminals, as well as the seizure of assets used in the commission of cybercrimes. After receiving complaints, the Center analyzes them. As the Center sees new threats emerge, it provides public service announcement about those threats. It also forwards complaints to the appropriate law enforcement agencies for further investigation. A complaint database maintained by the Center can be accessed by law enforcement personnel (see Federal Bureau of Investigation, 2018c). The Center itself has been the victim of cybercrime. In 2017, cybercriminals posed as the Center and sent e-mails to victims asking for personally identifying information. The cybercriminals claimed this was for the purpose of forwarding restitution to the victims. Victims were also sent a file they were asked to download to fill out with their personal information. The file was actually malware. The Center made the public aware of the scam in 2018 (Federal Bureau of Investigation, 2018a).

The FBI created its Cyber Division in 2002. The Cyber Division was created amidst a reorganization that was occurring at the FBI—and other federal agencies—due to the creation of the Department of Homeland Security following the September 11, 2001 terrorist attacks (Monroe, 2003). The stated purpose of the Cyber Division is to "address cyber crime in a coordinated and cohesive manner" (Federal Bureau of Investigation, 2019). The FBI certainly investigated cybercrime before the creation of the Cyber Division, but the creation of a specific division to address cybercrimes was done to make the process more effective. The Cyber Division not only investigates its own crimes, but assists both domestic and foreign agencies with their cybercrime investigations (Monroe, 2003).

Since the creation of the Cyber Division, the FBI has been involved in several notable cybercrime cases. In 2006, the FBI in conjunction with the Secret Service investigated CardersMarket—the largest English-speaking criminal marketplace on the internet at the time with a membership of roughly 6,000. The site was started by Max Vision—a computer security researcher that turned to hacking. Vision hacked other websites that trafficked in the personal information of others. Once he hacked those sites, he took that information for himself, then offered it through CardersMarket (Poulson, 2009). Vision was apprehended and ultimately sentenced to 13 years in prison.

In 2013, the FBI—along with the DHS and the Drug Enforcement Administration—was involved in the investigation and arrest of Ross Ulbricht (also known as Dread Pirate Roberts)—the owner and operator of the dark web marketplace Silk Road. Silk Road was being used by its members to sell drugs and other criminal contraband. One of the primary contributions of the FBI to the investigation was the locating of the servers that hosted Silk Road (Bearman et al., 2015). Ulbricht was sentenced to life in prison in 2015 for crimes arising from his involvement with Silk Road, including money laundering, computer hacking, conspiracy to traffic fraudulent identity documents, and conspiracy to traffic narcotics by means of the internet (Segall, 2015).

In 2015, the FBI was involved in Operation Shrouded Horizon. As part of that investigation with numerous international law enforcement agencies, agents were able to infiltrate an online black market known as Darkode that trafficked in malware, stolen identities, and other information to help facilitate cybercrimes. As part of that operation, the FBI was able to shut down the website and make arrests of cybercriminals in 20 different countries (Federal Bureau of Investigation, 2018b).

The FBI has also had to deal with cybercrime issues while investigating crimes that would not be considered cybercrimes. Perhaps most notably, the FBI ran into issues bypassing the security measures on a cellphone belonging to one of the suspects in the San Bernardino shooting in 2015. The FBI filed a motion to compel Apple—the maker of the phone—to bypass the security measures for them. The FBI was ultimately apple to bypass the security measures themselves, and the matter with Apple was never litigated (Selyukh, 2016). This case does serve as an example of how cyber technological issues can permeate the investigation of non-cybercrimes.

Cybercrime threats are ever-present. In the midst of these threats, the FBI has had difficulty retaining cybercrime employees. From 2013 to 2018, the FBI lost 20 of its top cyber security leaders. These employees left for higher paying jobs in the private sector. This included Scott Smith—the assistant direction of the FBI's Cyber Division, and Howard Marshall—Smith's deputy. This appears to be an issue the FBI will continue to deal with as long as cybersecurity continues to be as issue for businesses (Geller, 2018).

See also: Bypass; Child Pornography; Dread Pirate Roberts (Ulbricht, Ross; 1984–); Levin, Vladimir; Operation Innocent Images; Operation Shrouded Horizon; Silk Road

Further Reading

Bearman, Joshuah, Joshua Davis, and Steven Leckart. 2015. "The rise & fall of Silk Road, part 2." *Wired*, No. 23.6.

Federal Bureau of Investigation. 2018a. "Impersonation of the internet crime complaint center." Federal Bureau of Investigation. https://www.ic3.gov/media/2018/180201.aspx

Federal Bureau of Investigation. 2018b. "Major cases: Major cyber crime cases over the years." https://www.fbi.gov/investigate/cyber/major-cases

Federal Bureau of Investigation. 2018c. "2017 internet crime report." https://pdf.ic3.gov/2017_IC3Report.pdf

Federal Bureau of Investigation. 2019. "Cyber crime." https://www.fbi.gov/investigate/cyber

Geller, Eric. 2018. "FBI struggles to retain top cyber talent." *Politico*, August 3, 2018. https://www.politico.com/story/2018/08/03/fbi-cyber-security-talent-drain-hacking-threat-russia-elections-760740

Monroe, Jana D. 2003. "Before House Judiciary Committee, Subcommittee on Courts, the Internet and Intellectual Property." Federal Bureau of Investigation, July 17, 2003. https://archives.fbi.gov/archives/news/testimony/the-fbis-cyber-division

Poulson, Kevin. 2009. "The decade's 10 most dastardly cybercrimes." *Wired*, December 31, 2009. https://www.wired.com/2009/12/ye-cybercrimes/

Segall, Laurie. 2015. "Silk Road's Ross Ulbricht sentenced to life." CNN, May 29, 2015. https://money.cnn.com/2015/05/29/technology/silk-road-ross-ulbricht-prison-sentence/index.html

Selyukh, Alina. 2016. "The FBI has successfully unlocked the iPhone without Apple's help." National Public Radio, March 28, 2016. https://www.npr.org/sections/thetwo-way/2016/03/28/472192080/the-fbi-has-successfully-unlocked-the-iphone-without-apples-help

Suro, Roberto. 1999. "FBI lagging behind on cyber crime." *The Washington Post*, October 7, 1999. http://www.washingtonpost.com/wp-srv/national/daily/oct99/cyber7.htm

FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002

The Federal Information Security Management Act of 2002 (FISMA) is a U.S. law that creates a framework to protect government information, operations, and assets from cyber threats. FISMA is chapter 3 of the Electronic Government Act of 2002 (PL 107-347). The law was originally proposed because federal agencies are often targeted by cybersecurity attacks by individual cyber criminals or foreign governments. If criminals successfully breach the security of these sites, it can result in personal or sensitive data being stolen and/or made public. Representative Thomas Davis (R-VA) originally proposed the bill, and President George W. Bush signed it into law in December 2002.

The law requires federal agencies to develop, document and implement programs that provide information security for their systems. Federal agencies are also required to carry out annual reviews of their security plans, providing that information to the Office of Management and Budget (OMB), which in turn must report to Congress.

Specifically, the provisions of the law require that federal agencies:

1. Maintain and inventory of information systems that are maintained by that agency: or systems that interface between the federal agency and an outside agency;
2. Categorize information by the level of risk;
3. Develop and maintain a security plan for all systems; should be reviewed regularly;

4. Utilize security controls: organizations must meet minimum security requirements set by National Institute on Standards and Technology (NIST);
5. Conduct risk assessments to determine if additional controls should be added or if current ones should be changed.

If a federal agency chose to ignore the law, a judge was given a variety of penalties that could be applied to the offender. These include a Congressional censure, a reduction in federal funding, and damage to a person's reputation.

The regulations for increasing cyber security that were set forth by FISMA applied originally to all federal government agencies. The law was expanded to include to state agencies that carry out federal programs such as Medicare and Medicaid. Thus, some state agencies had to comply with FISMA regulations. Over time, FISMA was again expanded to increase oversight of the private sector. Currently, if a private-sector company has a contract with the government to provide a service or if it receives federal grant money, it must comply with FISMA.

The law makes it clear that FISMA agencies are still permitted to store data in the cloud, even though it poses a security risk. Agencies often turn to this form of data storage because it is cheap. If a cloud provider provides storage, it then becomes subject to FISMA regulations. To help with this, the government created the Federal Risk and Authorization Management Program (FedRAMP), a government program that gives a standardized program for security assessment, authorization, and monitoring of products that are held in the cloud. A cloud provider needs to show they are complying with FISMA if they comply with security standards and guidelines that have been developed by NIST, called the integrated Risk Management Framework. This is a statement of FISMA security standards to help agencies create their individual security plans.

Since being passed, compliance with FISMA has successfully increased the cybersecurity of sensitive federal data. Federal agencies and private companies have been able to create and maintain a higher level of security and lessen the chances of a security breach.

The original FISMA law was amended by the Federal Information Security Modernization Act of 2014 (44 U.S. Code § 3551; PL 113-283), sometimes referred to as FISMA Reform. This bill was S2521 and was signed by President Obama. As passed, the law requires less reporting, but it requires more reliance on continuous monitoring of systems to identify threats. The law also increases the compliance regulations and places an emphasis on problems that result after a security breach. It became necessary that agencies plan for security for their data and information so it remains safe. Part of this requires that employees are given the task of being responsible for the security of an agency. They must continue to review the security protocols in their agencies and revise them as needed. The bill also re-established the oversight powers of the Office of Management and Budget (OMB) for security policies and gave the DHS secretary the power to implement the security plans developed. The DHS now had the ability to carry out information security policies for civilian agencies, including the provision of technical assistance, among other things.

See also: Encryption; National Institute of Standards and Technology Cybersecurity Framework

Further Reading

Adams, Rebecca. 2006. "Data drip: How the feds handle personal data." *CQ Weekly*, July 10, p. 1846.

Lord, Nate. 2019. "What is FISMA compliant? 2019 FISMA definition, requirements, penalties and more." Digital Guardian, January 3, 2019. https://digitalguardian.com/blog/what-fisma-compliance-fisma-definition-requirements-penalties-and-more

Robinson, David, Harlan Yu, William P. Zeller, and Edward W. Felten. 2009. "Government data and the invisible hand." *Yale Journal of Law & Technology*, Vol. 11, p. 160.

U.S. Department of Homeland Security. Federal Information Security Modernization Act. https://www.dhs.gov/cisa/federal-information-security-modernization-act

FINANCIAL CRIMES

Generally speaking, financial crimes are crimes involving the misappropriation of the money of another. However, the precise definition of what constitutes a financial crime is not universally agreed upon. Some have a more expansive view of financial crime, extending the definition to include the misappropriation of any property of another (such as automobile theft), or to include any crime involving the handling of money (such as money laundering). Others may restrict the definition, categorizing property misappropriation crimes involving violence (such as armed robbery) differently than property misappropriation crimes that do not (see Jung and Lee, 2017; Pickett and Pickett, 2002). Even under its most basic definition, it is clear that financial crimes are able to be committed via cybermethods.

It has been suggested that financial crimes have several common elements. These include the use of deceit and the ability to conceal the crime (Jung and Lee, 2017; Pickett and Pickett, 2002). In regards to financial crimes committed via cybermethods, these elements are particularly pertinent. A cybercriminal wishing to commit a financial crime cannot can obtain money by physically taking it. Rather, they will have to gain access to a victim's money via an online bank account or other online financial account. Gaining such access will generally require the use of deceit. A cybercriminal may elicit personal information from the victim through some sort of fraudulent scheme (a phishing scheme, etc.). That information can then be used by a cybercriminal to access the victim's existing online financial accounts, or to start new accounts with that information—such as a credit card account—that could leave the victim stuck with a hit to their credit and potentially debt to pay off to the credit card company.

Cybercriminals are likewise simply not able to run away from a theft they have just committed to avoid detection. If they are not cautious, there is often a digital trail of the activities of a cybercriminal. Thus, a successful financial cybercriminal will have to somehow conceal their actions. Financial cybercriminals can use a virtual private network (VPN) service—a service that will mask your IP address while using a public internet connection. A similar tool that financial cybercriminals could use is Tor—software that also masks your IP address when using the internet. A masked IP address makes it difficult for law enforcement to track down the location from which a cybercrime was committed. Another tactic used is to infiltrate the computer of someone else and launch the cybercrime from there. In those instances, if law enforcement is able to track down the location the crime was committed from, it will be the computer of someone other than the actual cybercriminal. Financial cybercrimes may be launched from compromised computers of reputable organizations to more effectively lure in victims. This includes small businesses, public schools, and social clubs (Hackett, 2016). A tactic some cybercriminals might use to conceal themselves is the leaving behind of false flags—clues that appear to indicate who committed the crime, but actually lead law enforcement to someone other than the actual cybercriminal (Matsakis, 2018). After the funds of a victim are obtained, a cybercriminal can also launder those funds through cryptocurrencies to further obfuscate the trail.

The amount of financial crime that happens online is significant. Based on complaints made to the FBI, victims of online crime lost a total of $1.42 billion in 2017. The leading category of complaints the FBI received that same year was for failure to receive goods paid for, or not receiving payments they were entitled to. Other financial crimes that were frequently reported were credit card fraud, investment schemes, and sweepstakes schemes (Federal Bureau of Investigation, 2018). Financial institutions are particularly targeted by cybercriminals. Those companies are targeted by cybercriminals 300 times more frequently than other businesses. In 2017, financial institutions lost $16.8 billion collectively due to attacks from cybercriminals (Mirchandani, 2018). Many of the cybercrimes that occur are not, strictly speaking, financial crimes, but they do still result in monetary loss for the victims. Looking again at complaints made to the FBI by cybercrime victims, the crime reported that resulted in the most monetary loss for victims collectively in 2017 was having their e-mail account compromised. Having one's e-mail address compromised does not require the perpetrator to take money from the victim. However, the intent of the perpetrator is often to use that compromised e-mail address to someone deprive the victim of their money. Other frequently reported crimes that fall into this same category include identity theft, phishing schemes, and data breaches (Federal Bureau of Investigation, 2018).

Although there are certainly numerous ways to commit financial crimes, with large online financial crimes, there appear to be two general plans of attack for cybercriminals. One method is to attack an institution directly and steal money directly from it. This happened in 2015 when an international hacker group—the Carbanak cybergang—was able to steal nearly $1 billion from banks in 30 different countries, including the United States. The hackers were able to accomplish this by targeting the banks' employees with phishing attacks and gaining access to the inner working of the banks themselves (Kaspersky Lab, 2015; Snider and Whitehouse, 2015). Another method is to steal personal customer information from a large company and then use that personal information to steal money from customers individually after the fact. Several companies have been the victims of massive data breaches, such as Yahoo, Equifax, and Target. Customers whose personal information is compromised in these data breaches not only have to worry about that information being used to steal money from them, but in many instances, they must also worry about cleaning up fake accounts made by cybercriminals to defraud victims as well. This can take years for some victims to do (Hsu, 2017).

See also: Bitcoin; Cryptocurrency; Fraud; Hacker and Hacking; Identity Theft; Money Laundering; Phishing; Tor (The Onion Router)

Further Reading

Federal Bureau of Investigation. 2018. "2017 internet crime report." https://pdf.ic3.gov/2017_IC3Report.pdf

Hackett, Robert. 2016. "How hackers plan attacks and hide their tracks." *Fortune*, August 12, 2016. http://fortune.com/2016/08/12/how-hackers-hide-tracks-cyberattacks/

Hsu, Tiffany. 2017. "Data breach victims talk of initial terror, then vigilance." *New York Times*, September 9, 2017. https://www.nytimes.com/2017/09/09/business/equifax-data-breach-identity-theft-victims.html

Jung, Jeyong, and Julak Lee. 2017. "Contemporary financial crime." *Journal of Public Administration and Governance* 7, 2: 88–97.

Kaspersky Lab. 2015. *Carbanak Apt: The Great Bank Robbery*. Kaspersky Lab. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf

Matsakis, Louise. 2018. "To identify a hacker, treat them like a burglar." *Wired*, August 12, 2018. https://www.wired.com/story/case-linkage-hacker-attribution-cybersecurity/

Mirchandani, Bhakti. 2018. "Laughing all the way to the bank: Cybercriminals targeting U.S. financial institutions." *Forbes*, August 28, 2018. https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#2f4ac5b66e90

Pickett, K., H. Spencer, and Jennifer M. Pickett. 2002. *Financial crime investigation and control*. New York: John Wiley & Sons, Inc.

Snider, Mike, and Kaja Whitehouse. 2015. "Banking hack heist yields up to $1 billion." *USA Today*, February 15, 2015. https://www.usatoday.com/story/tech/2015/02/15/hackers-steal-billion-in-banking-breach/23464913/

FIREWALL

A firewall is an item used for computer security. It is designed to monitor traffic to and from a computer or computer network and to block traffic that does not comply with the security parameters in place (Cisco, 2019). A firewall can be used to protect a computer or computer network against cyberattacks.

Firewalls work by monitoring information coming through it, to and from the internet. Basic firewalls will gather information on the packets—broken-down bundles of data—being sent to and from the internet, such as the internet protocol (IP) address of where the data is coming from. The firewall is then designed to block any packets whose information does not comply with the parameters programed in the firewall, such as data that comes from an unauthorized IP address. More advanced firewalls will gather more information that can used to determine whether data should be blocked or allowed, such as the riskiness of an application (Cisco, 2019; Norton, 2019). These are sometimes referred to as intrusion prevention systems (IPSs). An IPS functions like an intrusion detection system (IDS), gauging network traffic patterns and blocking traffic that is abnormal for that network. While firewalls, IPSs, and IDSs are separate cybersecurity tools, the distinction between these tools has faded as technology has advanced and these tools incorporate aspects of the others (Bradley, 2019).

Firewalls can be either hardware or software. While both hardware and software firewalls carry out the same basic function, there are advantages and disadvantages to both. Hardware firewalls are generally easier to set up. A hardware firewall will generally be external to a computer. These may be built into another network device, such as a router. The design generally permits multiple computers to be run through it, providing protection to all those computers with no additional setup. While setup is easier, hardware firewalls only monitor incoming traffic, not outgoing. While this protects against many cyberattacks, it does not protect against all of them. Software firewalls, on the other hand, are able to monitor both incoming and outgoing traffic. The security parameters of software firewalls are also generally more customizable than hardware firewalls (Norton, 2019).

As alluded to above, although firewalls can help prevent many cyberattacks, there are ways to circumvent the security provided by them. Where firewalls block data based on information the firewall collects about that data, if a cybercriminal can find a way to falsify that information, they may be able to get data—such as malware—past the firewall. One way of doing this is spoofing. Spoofing is the process of making something appear that it is something it is not. For firewall circumvention, a cybercriminal would attempt to make a data packet appear to come from an IP address other than the one it is actually coming from in order to fool the firewall into letting it through. In this way, the spoofed data packets are working as a Trojan horse (Norton, 2019). Once the Trojan horse makes it through, the malware included inside can be downloaded to the targeted computer. Another similar method that can be used is the use of a virtual private network (VPN). A VPN can be used to hide the IP address of an internet user. While these can be used for privacy reasons, where the actual IP address of a user is hidden, a firewall would not block data sent or received from that user, even if their actual IP address was blocked. One type of cyberattack that may not be detected by a hardware firewall is the use of a bot. A bot is a computer that has been hijacked by a cybercriminal, allowing them to surreptitiously control that computer. As noted above, a hardware firewall is generally unable to monitor outgoing traffic from a computer. Thus, if a computer has been infected with malware and become a bot, a hardware firewall will be unable to monitor the outgoing activities a cybercriminal is initiating from that computer (Norton, 2019).

Installing malware is not the only reason that someone might want to circumvent a firewall. Firewalls are used by some countries to censor the material its citizens can access on the internet. This can be seen with the censorship apparatus in place in China, known as the "Great Firewall of China." Citizens in those countries can use the circumvention methods mentioned above to circumvent these firewalls and access censored material. In these countries, circumventing these firewalls or providing the means to circumvent these firewalls can be a crime.

See also: Bots and Botnets; China; Malware; Spoofing; Trojan Horse; Virtual Private Network

Further Reading

Bradley, Tony. 2019. "Introduction to intrusion detection systems." Lifewire, June 1, 2019. https://www.lifewire.com/introduction-to-intrusion-detection-systems-ids-2486799

Cisco. 2019. "What is a firewall?" https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Griffiths, James. 2018. "A software developer just became the latest victim of China's VPN crackdown." CNN, October 10, 2018. https://www.cnn.com/2018/10/10/asia/china-vpn-censorship-intl/index.html

Norton. 2019. "How does a firewall work?" https://www.nortonsecurityonline.com/security-center/how-does-firewall-work.html

FLORIDA COMPUTER CRIME ACT OF 1978

In response to a dog-racing betting scam, the Florida legislature passed the Florida Computer Crime Act in 1978, one of the first laws to create laws defining computer crimes. The law was in response not only to the scam at the race track but also to increasing computer crimes in both the public and private sectors—and the increase in costs that resulted from these crimes. Officials recognized that the opportunities that existed for computer-related crimes were very high, and there was a need for new, preventive action.

On August 30, 1977, Leon Rodriguez placed a bet at the dog track in Flagler, Florida. When the race ended, Rodriguez and four other people had won a jackpot of $15,000. Rodriguez had won legally, but the four other betters, who were "electronic partners," had won the money illegally through a computer scam. Under the scam, criminals made the losing tickets into winning bets by manipulating the computers that reported race results. Fraudulent winning tickets were then printed, and the winners cashed in their tickets the following day. The scam continued for many years, until the scam was discovered and the offenders arrested in 1977 (Hochman, 1986).

The content of the Florida Computer Crime Act includes regulations prohibiting the intentional modification or deletion of data or programs found on a computer. The law also makes it illegal to destroy or damage the hardware on a computer. A third provision makes it illegal to knowingly take or disclose data or documentation that is a trade secret or confidential. These offenses are all defined as offenses against intellectual property. These offenses are defined as a felony of the second or third degree, depending on the provision.

Another portion of the Florida law makes it illegal for an offender to willfully modify computer equipment or commit an offense against computer equipment. This can include acts such as destroying or damaging a computer system or network or destroying, damaging, or taking equipment or supplies. This is also defined as a third- or fourth-degree felony, depending on the damage caused by the destruction.

People who use computers were also given some protection under the law. According to the statute, any person who willfully or knowingly prevents a person from using a computer system that they are authorized to use will be guilty of a third-degree felony. If the offender commits the crime in an attempt to defraud a person or to obtain property, then it becomes a second-degree felony. By Florida law, a second-degree felony is punishable by a term of imprisonment of up to 15 years and a fine of up to $10,000, or a higher amount that is equal to double the profit the offender made from the crime or an amount that is twice the amount of the loss to the victim. A third-degree felony is punishable with a term of imprisonment of up to five years and a fine of up to $5,000 or higher, or an amount that is twice the profit gained by the offense or double the loss suffered by the victim.

If an offender is found guilty of committing a first-degree misdemeanor in the office, they may receive a punishment of up to one year in prison and a fine of up to $1,000. The fine may be larger, as it can be the amount equal to twice the profit gained from the offense or twice the loss suffered by the victim.

See also: CAN-SPAM Act of 2003; Computer Fraud and Abuse Act of 1986; Cybersecurity Act of 2012

Further Reading

Hochman, Marilyn. 1986. "The Flagler dog track case, 7 Computer L.J. 117." *The John Marshall Journal of information Technology & Privacy Law* 7, 1: 117–127.

UF Computing & Networking Services. 1999. "General information: Florida Computer Crimes Act. CNS document ID: D0010." www.security-science.com/pdf/general-information-florida-computer-crimes-act.pdf

414s

In 1982, a group of six teenaged boys between the ages of 16 and 22 from Milwaukee, Wisconsin, formed a computer hacking group called the 414s after the city's telephone area code. The boys were members of a Boy Scout–affiliated Explorer Post in the city that was sponsored by the International Business Machines Corporation (IBM). The company sought to teach the kids how to use new computers. The boys met weekly to discuss computer techniques and find ways to access computer games on different systems. To help them in their endeavor, they set up a type of bulletin board on which they could secretly leave each other tips and passwords, but they were also able to play computer games on these sites. The members soon began to hack into modems belonging to companies that were set up to give employees access to computers while they were traveling. The first three digits of these systems comprised the area code, followed by a second series of numbers. They were able to dial long distance without paying fees, a practice referred to as phreaking.

In time, the members hacked into the computer systems of many high-profile and government systems in the United States and Canada, including the nuclear weapons laboratory in Los Alamos National Laboratory in New Mexico, the

Sloan-Kettering Cancer Center in New York, a cement company in Montreal, and the Security Pacific National Bank. The boys became the first group of computer hackers and have been credited for bringing attention to the ease by which systems could be accessed and the need for better computer security. The members may have been acting out the events in the movie *WarGames* (1983), in which a teenage hacker breaks into nuclear defense computers. The movie was released at the same time the boys were carrying out their hacking activities.

Chen Chui, a systems manager for Sloan-Kettering, discovered the hacking by noticing the failure of a computer that monitored radiation treatment for patients. While looking into the event, he found that a file of billing records had been deleted and passwords issued for five new accounts. He contacted the Federal Bureau of Investigation (FBI), which then began an investigation and quickly discovered the activities of the 414 group. Some of the group members were Timothy Winslow, Gerald Wondra, and Neal Patrick.

One of the members, 17-year-old Patrick, became the public spokesman for the group. To defend and explain the group's activities, he was invited to be on the *Phil Donahue Show* (a popular talk show at the time). He also appeared on the cover of *Newsweek* magazine. He explained that the 414 members sought the challenge of breaking into the systems. They were having fun, simply looking for new computer games to play and had no intention of stealing information or selling it. They were able to do so fairly easily, using simple computers and basic hacking methods that were quite simple and could be used by many others. They used only their home computers and their telephone lines. Though the group had no intention of causing damage, they were the cause of financial harm. Sloan-Kettering claimed the group caused $1,500 in damages because they deleted billing records as they tried to hide their intrusion.

As the related events became more widely known, the public and company officials recognized the vulnerabilities of computers and systems. They came to the realization that more needed to be done to protect their systems and their data. After it was discovered that the username and password for the Memorial Sloan-Kettering Cancer Center were both "test," the need for better passwords and more secure technology became evident. Many companies made changes to improve their security and patched potential access points to their systems.

In the end, the 414 members were not prosecuted, partly because some were minors but also because there were no laws banning hacking at the time. The members agreed to stop their hacking activities and pay restitution to the companies they hacked. Two members were convicted of misdemeanor charges of making illegal or harassing phone calls across state lines (because they used a system called Telnet that connected computer terminals to each other). These offenses at the time were punishable by a maximum term of six months in prison and a fine of $500. The government offered the boys a plea deal under which they were placed on two years of probation and fined $500. Under the Federal Youth Corrections Act passed in 1950, their records would be expunged.

In 1983, Patrick was asked to testify in front of the U.S. House of Representatives about computer security and hacking, and six new federal laws were proposed and passed to deter cybercrime. One of those laws was the Computer Fraud and Abuse Act, which Congress passed in 1984. Under this law, it became illegal to knowingly access a computer without authorization or by exceeding access that has been granted. It became a federal offense to knowingly access a computer with the intent to defraud and obtaining anything of value or to cause damage to files (which the 414s did). The law also banned intentionally accessing any private computer system of a U.S. agency or department.

In 2015, a documentary movie was made of their activities. Called *The 414s: The Original Teenage Hackers*, the 12-minute film was directed by Michael Vollmann and produced by Chris James Thompson. It was launched at the Sundance Film Festival in 2015 and then shown on CNN. One of the hackers, Timothy Winslow, eventually became a network engineer.

See also: Computer Fraud and Abuse Act of 1986; Hacker and Hacking

Further Reading

Elmer-DeWitt, Philip. 1983. "Computers: The 414 Gang strikes again." *Time*, August 29, 1983. http://www.time.com/printout/0,8816,949797,000.html

Middleton, Bruce. 2017. *A history of cyber security attacks: 1980 to present*. Boca Raton, FL: CRC Press.

Schumacher, Mary Louise. 2015. "Milwaukee's original teen hackers focus of film premiering at Sundance." *Sentinel Journal*, January 20, 2015. http://archive.jsonline.com/entertainment/movies/milwaukees-original-teen-hackers-focus-of-film-premiering-at-sundance-b99429647z1-289228761.html

Storr, Will. 2013. "The kid hackers who starred in a real-life WarGames." *Telegraph*, September 16, 2013. http://www.telegraph.co.uk/film/the-414s/hackers-wargames-true-story/

Winslow, Timothy. 2016. "I hacked into a nuclear facility in the 80s. You're welcome." CNN Films, May 3, 2016. https://www.cnn.com/2015/03/11/tech/computer-hacker-essay-414s/index.html

FRAUD

Broadly speaking, fraud is "[a] knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment" (Garner, 2001). Fraud can be criminalized generally. Criminal law in the state of Arizona contains such a statute, making it a crime to "knowingly [obtain] any benefit by means of false or fraudulent pretenses, representations, promises or material omissions" (ARS § 13-2310). Specific types of fraud can be separately criminalized as well. Examples of this in federal criminal law include a credit card fraud statute (15 U.S. Code § 1644), a securities fraud statute (18 U.S. Code § 1348), and a computer fraud statute (18 U.S. Code § 1030). Fraud can also be an element of other crimes. For example, California's rape statute includes a provision criminalizing sexual acts that occur through intentional fraud on the part of the perpetrator (California Code, PEN § 261). Given the broad definition of fraud and the multitude of instances in which it can be used, it would be incorrect to categorize it strictly as a financial crime. However, fraud is often employed for the purpose of illegally depriving someone of their money.

Fraud can be committed as a cybercrime. As noted above, computer fraud specifically is a crime in some jurisdictions. Even in those jurisdictions without a specific computer fraud statute, a cybercriminal can still be found guilty of fraud under a general fraud statute. For many financial crimes online, cybercriminals will have to employ some sort of fraud to complete the crime. This stems from the nature of cybercrime. A cybercriminal will not generally have the ability to simply take an item away from someone as may be the case with some noncyber thefts. In order to misappropriate someone else's money online, a cybercriminal will first have to gain access to that money. To accomplish this, some level of fraud will generally be necessary.

There are some common methods by which cybercriminals use fraud to obtain money from their victims. According to the FBI, one common method used by cybercriminals in 2017 was to compromise business e-mail addresses (Federal Bureau of Investigation, 2018). A cybercriminal can compromise a business e-mail address either through social engineering or hacking. After the e-mail address has been compromised, a cybercriminal can use that e-mail address to surreptitiously transfer funds out of the business. It could also be used—while posing as a legitimate employee within the business—to ask other employees for personally identifying information, such as that included in payroll or tax withholding records. Another common method mentioned by the FBI is tech support fraud. In these cases, cybercriminals will poses as tech support personnel for a company. The cybercriminals contact victims purporting to offer assistance to the victim with made-up problems, such as a compromised e-mail account, resolving issues with their cable television, or resolving issues with their bank account. If the victim believes the cybercriminal is in fact a legitimate tech support employee, they can unwittingly provide personally identifying information to the cybercriminal, enabling them to access and take the victim's money.

There are additional fraudulent methods a cybercriminal might use. A cybercriminal may create a false online presence and attempt to lure in a victim through romantic overtures—a practice known as catfishing. Once a victim believes the romantic relationship is legitimate, the cybercriminal will concoct a financial difficulty and ask the victim for money. Another quick method used by cybercriminals is "Can you hear me?" calls. In that scheme, a cybercriminal will call potential victims and ask "Can you hear me?" If a potential victim responds, their voice is recorded by the cybercriminal. That recording can be used as a voice signature to authorize money transfers over the phone (Tatham, 2019).

Cybercriminals are constantly evolving, and they take their schemes to where people are online. An example of this is the increase in financial cybercrimes in the popular video game Fortnite, which had 200 million users as of late 2018. The game is free to play, though players can purchase additional items in the game (character skins, dance moves, etc.) with V-Bucks—the in-game currency which generally requires actual currency to purchase. Cybercriminals will offer free V-Bucks to players, the condition being that the victims must first provide personally identifying information to the cybercriminal. As a good number of those playing the game are children, it appears as though cybercriminals are trying to target a vulnerable population who may not be as able to notice the signs of a fraud scheme (Sun Reporter, 2018).

See also: Financial Crimes; Hacker and Hacking; Identity Theft; Phishing; Social Engineering

Further Reading

Federal Bureau of Investigation. 2018. “2017 internet crime report.” https://pdf.ic3.gov/2017_IC3Report.pdf

Garner, Bryan A. 2001. *Black’s Law Dictionary*. 2nd Pocket Edition. St. Paul, MN: West Group.

Sun Reporter. 2018. “Fortnite V-Bucks scam warning issued by police as gamers lose THOUSANDS to fraudsters.” *The Sun*, October 5, 2018. https://www.thesun.co.uk/tech/7425496/fortnite-scam-free-vbucks-police-warning/

Tatham, Matt. 2019. “The Ultimate List of the Year’s Worst Scams.” *Experian*, March 11, 2019. https://www.experian.com/blogs/ask-experian/the-ultimate-list-of-the-years-worst-scams/

G

GAMBLING

Gambling is the playing of games of chance for money. The laws regarding gambling differ from state to state. Perhaps the most extreme examples can be seen in the neighboring states of Utah and Nevada. Utah prohibits almost all forms of gambling. It does not even have a lottery. Nevada, on the other hand, allows casinos throughout the state. Another level of complexity is added to this when taking Native American reservations into account. Establishment of casinos is permitted on reservations (25 U.S. Code § 2701 et seq.), and thus a state that does not permit casinos might find a casino within its borders if a reservation within its borders establishes one.

With the advent of the internet, gambling has moved online. Because gambling websites are accessible from any state (or any country for that matter), online gambling can be tricky to operate and regulate. States are split on how to handle online gambling. Only a handful of states permit some form of it. The United States has also faced issues regulating online gambling that is hosted in foreign countries and occurs in the United States. On March 13, 2003, the country of Antigua filed a complaint against the United States with the World Trade Organization over the United States's handling of online gambling from other countries. This complaint stemmed from a criminal cases in the United States filed in 2001 against Jay Cohen—one of the founders of a company involved in online gambling known as World Sports Enterprise. World Sports Enterprise was licensed to operate in Antigua in 1997, and it was the second largest employer in Antigua. The criminal complaint against Cohen was for accepting bets in Antigua from jurisdictions in the United States where gambling was illegal. Cohen was convicted and sentenced to 21 months in prison. Following this case, Antigua's online gambling business dropped. The complaint filed with the World Trade Organization claimed that the United States was impermissibly stifling Antigua's legitimate business in violation of obligations the United States had under a World Trade Organization treaty. The Organization agreed. This ruling would seemingly restrict the United States from limiting legitimate online gambling sites that are hosted in a foreign country from operating within the United States (Pontell et al., 2011).

One of the arguments that comes up with gambling is whether or not the game in question is a game of chance or a game of skill. Again, depending on the state, placing bets on a game of skill might be legal in places where placing bets on a game of chance may not be. A game of chance is one where the outcome of the game is completely random (i.e., left to chance). A game of skill, as the term implies, requires some level of skill in determining the outcome of the game. For example, a state lottery would be a game of chance because the numbers are chosen completely at random. Conversely, billiards would be a game of skill as the outcome is based on the skill of the players. There are a host of games that fall somewhere in between these two extremes. There can be debate whether games fall more on the side of chance or more on the side of skill. Poker is one such game over which this debate occurs. There is certainly chance built into the game, as players are randomly dealt cards. However, there is skill involved as well, because players are required to calculate their odds of winning a given hand, read their opponents to try and ascertain how strong their hand might be, and then determine how much to wager. At least one judge has determined that it is a game of skill (Secret, 2012).

There are online-specific games where this same debate is waged. Daily fantasy sports falls into this category. Daily fantasy sports allow players to create a fantasy team in their sport of choice (e.g., football, basketball, baseball) for the day within a bracket with other players. There are fees charged to play. The winner of a bracket gets the money. Companies that allow betting on daily fantasy sports argue it is skill-based as it requires knowledge of players within the professional sport they are betting on. The counterargument is that an individual player's performance on a day-to-day basis is more a matter of luck.

There is some concern over the fairness of online gambling. This may stem from the fact that those playing these games do not get to directly see the people they are interacting with. This can lead to distrust of the website hosting the online gambling (e.g., claiming the dealing of cards is not truly random in online poker) or distrust of those they are playing with (e.g., fears that other players of the game are actually just different accounts being controlled by the same person to give them an edge in the game). There have been lawsuits filed against online gambling sites for fraudulent practices. Several online gambling sites have had employees use the sites and gamble against customers. Online poker site Absolute Poker had an employee hack into the system to be able to see opponents' cards, and the employee won at least $400,000 doing so (Brunker, 2007). Daily fantasy sport sites Fan Duel and Draft Kings had employees of their sites gambling via the competitor's site, potentially using analytic information that their own company had produced. This use of non-public information to win on a competitor's site was of concern (see Rovell, 2015). Fan Duel and Draft Kings were also accused of false advertising, making claims that average players could win big using these gaming sites (Rovell, 2015).

See also: Financial Crimes; Fraud

Further Reading

Brunker, Mike. 2007. "Online poker cheating blamed on employee." *NBC News*, October 19, 2007. http://www.nbcnews.com/id/21381022/ns/technology_and_science-security/t/online-poker-cheating-blamed-employee/#.W8olXntKiM8

Pontell, Henry N., Gilbert Geis, and Gregory C. Brown. 2011. "Internet gambling." In *Cyber criminology*, edited by J. Jaishanker. Boca Raton, FL: CRC Press, pp. 13–28.

Rovell, Darren. 2015. "Class action lawsuit filed against DraftKings and FanDuel." ESPN, October 9, 2015. http://www.espn.com/chalk/story/_/id/13840184/class-action-lawsuit-accuses-draftkings-fanduel-negligence-fraud-false-advertising

Secret, Mosi. 2012. "Poker is more a game of skill than of chance, a judge rules." *New York Times*, August 21, 2012. https://www.nytimes.com/2012/08/22/nyregion/poker-is-more-a-game-of-skill-than-of-chance-a-judge-rules.html

GAMEOVER ZEUS BOTNET

GameOver Zeus was a sophisticated piece of malware that was first discovered in 2011. It was used by cybercriminals to steal banking and other credentials from victims. The Botnet was spread primarily via spam e-mail or phishing messages. A victim received an e-mail that appeared to be from a bank and opened an attachment, which immediately downloaded malware onto the computer that allowed the offenders to control the computer. Once the hackers had access, they were able to steal the victim's banking credentials or other personal information. They would then use that data to transfer money from the victim's accounts into accounts controlled by the criminals. In some cases, the hackers also used a DDoS attack that would distract the victim from the GameOver Zeus attack.

An infected computer, called a bot, would become part of a global network of infected compromised computers, also called botnets. The FBI estimated that the GameOver Zeus botnet was responsible for the theft of millions of dollars from individuals and businesses, not only in the United States but also globally (FBI, 2014).

The GameOver Zeus botnet was also the means by which a malware called Cryptolocker was spread. This malware encrypted the data on a computer and prevented the owner from accessing any data or files until it was unencrypted or unlocked by the criminal. The offender demanded a payment (usually in Bitcoins) from the victim before they would unlock the files. This type of malware is called "ransomware" and is becoming a popular form of malware. It had been estimated that Cryptolocker was responsible for infecting over 234,000 computers, with over $27 million in ransom payments (FBI, 2014).

In June 2014, officials in the U.S. Department of Justice and the FBI announced they would conduct an investigation in cooperation with international law enforcement agencies to discover who was responsible for the botnet. That same month, in Operation Tovar, the FBI seized control of the networks used by the criminals to infect the computers. Other agencies involved in the investigation were Europol, the European Cybercrime Center (EC3), and the National Crime Agency from the United Kingdom. Also participating in the investigation were security firms including CrowdStrike, Dell, Symantec, and McAfee. At about the same time, officials in other countries (Canada, France, Germany, the United Kingdom, and others) took over servers that the offenders used to spread the virus. Together, they were able to reroute the traffic to a safe, government-controlled computer that removed the virus from the infected computer.

In July 2014, the Department of Justice declared that they were bringing criminal charges against the person who served as the administrator for the botnet, Evgeniy Mikhailovich Bogachev, from the Russian Federation. The FBI identified Bogachev as a major cybercriminal who also went by the name Lucky12345. He is currently on the FBI's Cyber Most Wanted List for the following charges: Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud. The Department of Justice is offering a $3 million reward for information leading to Bogachev's arrest and/or conviction.

See also: Bitcoin; Bots and Botnets; European Cybercrime Center; Federal Bureau of Investigation; Malware; Phishing; Ransomware

Further Reading

Apuzzo, Matt. 2014. "Secret global strike kills 2 malicious web viruses." *New York Times*, June 3, 2014. https://www.nytimes.com/2014/06/03/world/europe/battling-destructive-computer-viruses-agents-seize-networks-used-by-hackers.html.

FBI Most Wanted: Evgeniy Mikhailovich Bogachev. https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev

Federal Bureau of Investigation. 2014. "GameOver Zeus botnet disrupted: Collaborative effort among international partners." June 2, 2014. https://www.fbi.gov/news/stories/gameover-zeus-botnet-disrupted

Krebs, Brian. 2014. "'Operation Tovar' targets 'Gameover' ZeuS Botnet, CryptoLocker scourge." Krebs on Security (blog), June 2, 2014. https://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/

Nakashima, Ellen. 2014. "Governments, security firms coordinate secret operation to dismantle GameOver Zeus botnet." *Washington Post*, June 3, 2014. https://www.washingtonpost.com/

U.S. Department of Justice. 2014. "U.S. leads multi-national action against 'Gameover Zeus' botnet and 'Cryptolocker' ransomware, charges botnet administrator." U.S. DOJ Office of Public Affairs, June 2, 2014. https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware

GLOBALHELL (gH)

globalHell, or gH, is a "cybergang" founded by Patrick Gregory, a member of a street gang who went by the name "MostHateD." The group became sophisticated computer hackers but had many of the same characteristics of a gang, such as the organizational structure. They also carried out some of the same activities as a gang, including trafficking in stolen credit card numbers. The members were also known for hacking into the websites of high-profile organizations, including the FBI, the White House, the interior department, the Senate, and the state of Virginia. They also hacked the websites of corporations and private organizations. After hacking into a company's business, Gregory threatened the company by telling them to pay a ransom, or he would destroy the business. After doing this, Gregory and other members boasted about their actions, bringing attention to what they did.

The members of the group started to steal conference-calling codes, and with that information, they created illegal conference calling "bridges." This allowed hundreds of hackers to speak to each other simultaneously. However, members forgot to disable the recording device, giving investigators a record of all of their conversations. On May 9, 1999, police executed search warrants on 16 members of the organization. The remaining members of the group hacked into and then damaged websites as a way to show support for those who were taken into custody. One of the sites damaged belonged to the FBI. The attack caused thousands of hits, shutting down the site.

Gregory, a 19-year-old from Houston, Texas, was charged with computer hacking, and he faced up to five years in jail and a fine of $250,000. He agreed to cooperate with police in exchange for a possible reduced sentence. At the same time, two other members of the group were convicted of committing various computer crimes. One of those members was 19-year-old Eric Burns, also known as Zyklon, from the state of Washington. He pleaded guilty to defacing the White House website. Burns was also banned from using a computer for a three-year period. In addition to hacking into the White House website, Burns was able to hack into the websites for the North Atlantic Treaty Organization (NATO), a U.S. embassy, and Vice President Al Gore. He hacked into the site of the U.S. Information Agency (USIA), causing the agency to shut the site down for eight days. Burns said of the attack, “I didn’t really think it was too much of a big deal” (CBS News, 1999).

The second member of the group who was convicted was Chad Davis, a 20 year old from Wisconsin who also went by the moniker “Mindphasr.” Davis was sentenced to six months in jail and three years of supervised release for defacing the website of the U.S. Army. He was able to replace the homepage for the Army with a message that said “Global Hell is alive. Global Hell will not die.”

After the members of the group were arrested, other members protested the action by hacking into the websites of the White House and the U.S. Senate. The sites were then defaced. No information was stolen, and it appeared that the goal was simply to embarrass the owners.

At its peak, globalHell included about 60 members, but the organization broke up in 1999 after 12 of the members were prosecuted. In all, members of the group destroyed data on 115 websites, causing between $1.5 and $2 million in damages.

See also: Department of Defense, Attacks on; Federal Bureau of Investigation; 414s; Hacker and Hacking; Legion of Doom

Further Reading

CBS News. 1999. “White House hacker faces jail.” November 23, 1999. https://www.cbsnews.com/news/white-house-hacker-faces-jail/

Goldman, John J. and Ush Lee McFarling. 2000. “Man accused of hacking into NASA computers.” *Los Angeles Times*, July 13. 2000. http://articles.latimes.com/2000/jul/13/news/mn-52233

Simons, John. 1991. “FBI sting targets computer hackers.” *Deepdyve*, January 1, 1991. https://www.deepdyve.com/lp/elsevier/fbi-sting-targets-computer-hackers-D7M9BYqnf9

Suro, Roberto. 1999. “The hackers who won’t quit.” *The Washington Post*, September 1, 1999. http://www.washingtonpost.com/wp-srv/national/daily/sept99/global1.htm

ZDNet UK. 2000. “Global Hell hacker to plead guilty, part 1.” March 30, 2000. https://www.zdnet.com/article/global-hell-hacker-to-plead-guilty-part-i/

H

HACKER AND HACKING

A hacker is a person who uses their computer skills to access another person's or organization's computer system or network without permission or authorization. They will intentionally breach a network's security system. Once in a system, a hacker may try to modify or change a system's hardware or software so that it can be used for another purpose, or so they can control what the computer does. A hacker may upload malware so they can steal information from the user or the company, or to modify the content of a website. Some hackers intend to take confidential business operations or proprietary information from another business, possibly a competitor. Some hackers plan to deface a website, launch malware, or destroy systems altogether.

Hackers often focus on businesses, attempting to either cause damage to the company or to steal secrets. However, government sites are often the targets of a hacking attack. This is because many sites have sensitive information, such as personal information or military secrets. A hack into one of these sites can affect thousands or even millions of people. If the hackers who access a government site have the support of a government, they are referred to as nation-state-sponsored actors.

There are many reasons why a person would want to hack into another's computer system. Hackers may be motivated by revenge. They may be a former employee who seeks to cause harm to a company's reputation, or they may be opposed to big business. These hackers may blackmail companies, steal credit card information, or use ransomware. Other hackers are motivated by a desire to harm others, so they may seek to release personal information or embarrassing e-mails that will cause not only embarrassment but harm the victims' careers. Some hackers are motivated by financial gain and seek to steal financial information or credit card numbers.

Some hackers choose to gain access to a site for political reasons. They may seek to deface the site of a large corporation, for example, to denounce their business practices. Or they may seek to encourage political action or activism. These hackers are referred to as "hacktivists" and their actions called "hacktivism." The words are a combination of activism and hacking. These hackers will sometimes want to deface websites, or they may want to steal information that is embarrassing to the company and publish it. This may be not only embarrassing to the organization but also harmful in some cases.

Some hackers may be interested in the fame they may receive after successfully hacking into a site and see it as a way to bolster their status within the hacking community. It can be difficult to know much about hackers and their activities because they don't want to be known. Many hackers could face criminal punishments if their activities are made public.

A large number of hackers simply find it a challenge to break into a secure system, and do it for fun. They see it as a way to test their knowledge of technology and as a way to improve their understanding of computers. They want to stay on top of changes in technology and want to know how things work. They find hacking to be exciting and entertaining.

Typically, a hacker has an expertise in computers and hacks into a system using that expertise. They must be proficient in computers and technology in order to find ways into a network. However, a hacker can use other methods to get into a system. They can "shoulder surf" or simply look over a user's shoulders to obtain their passwords or personal information. Or they can use social engineering to try to convince people to provide them with information so they can access websites. A hacker may contact a user and convince them that they work for an IT department, luring them into providing their password or personal information. They can use that information to gain access to files.

Although many hackers are able to use their own skills to break into a computer system, not all people who seek to be hackers have the knowledge to do this. They are unable to create the malware programs they want to use to discover vulnerabilities in other's systems. If a potential hacker is unable to write their own code, they can use premade malware that is available for sale on the internet or the dark web.

White Hat and Black Hat Hackers

A white hat hacker is a category of computer hacker who does not have the intent to harm the computer network or steal data. They are "good guys" who seek to access computer systems illegally simply to learn more about them. They are often security experts who seek to discover security issues or people who just want to know how the system works. They enjoy fixing or modifying things, and they hack simply because they enjoy the challenge. White hat hackers typically have an expertise in computers and have better computer skills than most people. They may be hired by a company or organization to test their own security systems. The hackers try to find weak points or vulnerabilities in their systems so preventive action can be taken before an attack occurs.

A black hat hacker, on the other hand, is a person who has great knowledge of computers and who seeks access to a system by bypassing security for criminal reasons or for profit. They may also do so for political reasons. Once they have access to a system, they may do things like steal data or other material, personal information, or credit card information. They may also destroy or alter files or steal trade secrets.

Hacker Subculture

While many hackers enjoy working individually, others come together in hacking communities where they can provide support to each other. They can communicate with other hackers and share expertise with one another. The members give hackers the opportunity to discuss hacking techniques or even events, problems, and issues if they arise. Some hackers will share hacking codes or malware that others can use. Hackers will also maintain communication and contact with other hackers through journals and conferences.

Most of the time the communication is done with secrecy to hide the participants' identity, not just from each other but also from law enforcement. That means that the hackers will use code names in place of their real names. Many participants in the hacking community, therefore, do not know each other's real identities.

The term given to this phenomenon is "hacker subculture." It refers to the process whereby like-minded individuals who enjoy computer programming, information technology, hacking and the like come together. Three norms or characteristics have been linked to the hacker community: technology, knowledge, and secrecy (Holt et al., 2018). The first of those, technology, refers to the interest that hackers have in computer software and hardware as well as other devices, including video games and cell phones. Through their hacking behaviors, those in the community seek to develop their technical skills and then apply what they know to existing technology.

The second norm, knowledge, refers to the overall knowledge that hackers have regarding technology and computers. Hackers tend to spend a great deal of time learning more about technology. They often will do that on their own, often by hacking, but new sites have been developed as a place for hackers to share videos and tutorials to demonstrate new hacking techniques.

The third norm of the hacking community is secrecy. Hackers tend to take actions that will keep their identity secret, largely because their behaviors are illegal. They will often use nicknames to refer to themselves in their communication with others. This way, no one knows who they are. Research into the hacking community shows that most hackers are usually young, under the age of 30.

Effects

Hacking can sometimes be very destructive to the victims. Hacking may cause the victim to suffer from economic losses due to a defaced website or resulting negative publicity. Companies have had intellectual property and trade secrets stolen, resulting in economic damage. There may also be psychological impacts or social consequences after the release of personal information that is embarrassing. Some victims have had their credit card numbers stolen and bank accounts hacked, resulting in a loss of thousands of dollars. Some companies have to pay for damages or losses to their customers in light of hacking actions. Hackers have stolen military information that could be dangerous to the nation's security.

There are many examples of hacking that has caused damage to a company. One of those was the 2014 hacking of SONY Entertainment. Hackers who called themselves the "Guardians of Peace" entered the computer systems, defacing the screens displayed to employees. The hackers took control of the company's Twitter accounts, demanded money, and threatened to "bombard" the company if the money was not sent. Probably most damaging, however, was the release of confidential documents that made public various company secrets, including embarrassing e-mails sent to and from top executives, as well as private employee information.

There have been multiple instances of hacktivism. One of those was against Republican Senator Pat Toomey, from Pennsylvania. He announced that his campaign organization was the target of an attempted hack in which people attempted to access his e-mails. This was accomplished through a failed phishing scam. Russian-based groups hacked the Democratic National Committee during the 2016 presidential campaign. Hackers also attempted to access Missouri Senator Claire McCaskill's accounts in February 2018, as well as those of Senator James Shaheen of New Hampshire.

Steven Branigan identified seven steps needed to perform a successful hacking. The first step is to select a target. This depends in part on the goal or aim of the individual hacker. If the hacker seeks financial gain, then an appropriate target would be a site that has a database of credit card information. If the hacker's goal is to attain publicity, then they should choose a popular site that many people rely on. However, if the hacker seeks to access a site just for the challenge, then the target site should be one that is challenging. The second step is to locate computers of the target that may be accessible to the hacker, either through the internet or a modem. It is essential that the hacker locate computers that are accessible; otherwise, the attack cannot be implemented (Branigan, 2005).

The third step is to discover any vulnerabilities or backdoors in the security systems of the target sites. The site may have particular times when they are less secure. There are many tools that are available for identifying potential vulnerabilities that are available for purchase or rental on the dark web, sometimes for a relatively low price. The fourth step in a hack is to break into the computer system by use of hacking tools, or to gain access to the system in some fashion. This can be done with an individual's technical expertise or with tools that are available on the Internet. This can also be accomplished through social engineering techniques, as described above (Branigan, 2005).

Once a hacker is in to the system, the fifth phase is to elevate any computer access privileges to the highest level possible. This is a necessary step so that the hacker has access to the greatest amount of data possible, or the "most secret" data that typically is accessed by the fewest number of people. This process is referred to as "rooting a box." After this, the hacker should seek to find any additional vulnerabilities that will provide him or her with additional access, or access to other computers. And finally, the hacker should install a backdoor, which is a way to maintain access to the site. It allows a person to return and reenter the system at a later time. This is an important step. If the people overseeing the targeted site discover the breach, they may patch the original vulnerability. A backdoor will give the hacker the ability to access the site even if the vulnerability is fixed (Branigan, 2005).

See also: Black-Hat Hacker; Cracker and Cracking; Hacktivism; Sony Pictures Entertainment Hack; White-Hat Hackers

Further Reading

Benjamin, Victor, Sagar Samtani, and Hsinchun Chen. 2017. "Conducting large-scale analysis of underground hacker communities." In *Cybercrime through an interdisciplinary lens*, edited by Thomas J. Holt. New York: Routledge, pp. 56–75.

Branigan, Steven. 2005. *High-tech crimes revealed*. Boston, MA: Addison-Wesley.

Holt, Thomas J. 2009. "Lone hacks or group cracks: Examining the social organization of computer hackers." In *Crimes of the internet*, edited by F. Schmalleger and M. Pittaro. Upper Saddle River, NJ: Pearson Prentice Hall, pp. 336–355.

Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. 2018. *Cybercrime and digital forensics*. New York: Routledge.

Steinmetz, Kevin F. 2015. "Crafty(y)ness: An ethnographic study of hacking." *British Journal of Criminology, 55*, 125–145.

Turgeman-Goldschmidt, Orly. 2008. "Meanings that Hackers assign to their being a hacker." *International Journal of Cyber Criminology* 2, 2: 382–396.

Wade, Cassie, Jessica Aldridge, Lindsay Hopper, Holli Drummond, Ronald Hopper, and Keith Andrew. 2011. "Hacking into the hacker: Separating fact from fiction." In *Crime online*, edited by Thomas J. Holt. Durham, NC: Carolina Academic Press, pp. 29–55.

HACKTIVISM

Hackers who access a computer network that belongs to another person without their permission for ideological, religious, or political reasons are referred to as hacktivists. Individuals use typical hacking techniques as a way to promote their agendas or to promote their opinions, and try to convince others to support their cause. For the most part, the activities of hacktivists do not cause fear—their acts are not considered to be terrorist acts. Instead, they are acts of protest or political action and expression.

Hacktivists use many techniques as they attempt to promote their agenda. One is simply to hack into a computer system and deface a website. They may post inaccurate information or messages from their organization. Other hacktivists choose to access files and steal personal information, e-mails, or records and then publish them as a way to embarrass those involved. This happened in the 2014 attack on SONY Entertainment, when confidential e-mails from executives were published that contained racist or offensive remarks. Some hacktivists rely on denial-of-service attacks through which they are able to take a website offline. Another technique is "doxing" through which the hacktivists gather background information on a particular individual and post it online. Much of the information posted can be not only embarrassing to the individual, but also to family members. It can also discredit the person who is targeted. If personal addresses are posted online, it can result in physical harm to the victim.

Some hacktivists may see their actions as a form of social protest; however, online attacks are criminal acts. They can be disruptive to a business or government office and can be harmful to a business or agency. It can be costly to any victim, as an agency or company must pay for the costs related to addressing any damage done by the attack. They must also pay for additional software or technology that is needed to prevent any future attacks. For businesses, this money comes from profits; for government offices, this money comes from taxpayers. Sometimes the effect on the public's trust in that organization, whether it be a business or government office, can be devastating.

Hacktivism is not a new phenomenon. In the 1980s and 1990s, a group called Cult of the Dead Cow (cDc) encouraged hacking by their members and others. Group members from Lubbock, Texas, included Swamp Ratte (otherwise known as Grandmaster Ratte), Franken Gibe, and Sid Vicious. Their goal was "global domination through media saturation." The members of cDc encouraged hacking behaviors by others and also supported acts of hacktivism to further their political purposes. To support hacktivism by those less experienced in computers, the group made hacking tools more readily available. These included Back Orifice (BO) and Back Orifice 2000 (BO2K), Trojan Horse malware that allows people to gain remote access to infected computers running the Microsoft Windows operating system. They continue to develop privacy and security tools for the Internet and publish a magazine called *Cult of the Dead Cow* that was originally published in the 1980s.

Members of cDc took advantage of infighting that was taking place on between other hacking groups to grow into a larger, more easily recognized group. It quickly became known for its use of humor in its activities. Members often wore clothing with humorous depictions that outsiders sometimes found offensive, such as pictures of a crucified cow. While members of other hacking groups (LOD and MOD) were arrested and indicted for their hacking activities, cDc members were able to evade law enforcement. It has been reported that Democratic presidential candidate Beto O'Rourke was a member of cDc while a teenager in Texas. His exact role in the group is not fully known.

Another hacking group that supports hacktivism is Anonymous. The members of this group have a history of attacking sites belonging to governments, businesses, and even religious organizations. They have attacked the Church of Scientology, the Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA), and the BART subway system in San Francisco after the police shot an unarmed passenger in 2009. Members of Anonymous launched an attack on the state website in Missouri after the shooting of Michael Brown, an unarmed black teenager in August 2014 in Ferguson. Members of the group used a DoS attack and doxed various officials. The websites were brought offline for brief times but state IT experts were able to bring them back online quickly.

In December 2010, a group of hacktivists who went by the name "Operation Payback" hacked into PayPal, Visa, and MasterCard sites and launched a DoS attack that took the sites down for a short time, preventing customers from accessing their accounts. These attacks were in retaliation for the companies' decisions to break their support of WikiLeaks after it published top secret documents. The website of the television station PBS was also defaced after it ran a show that was unfavorable of WikiLeaks. It wasn't long before arrests were made in the attacks. The offenders were all young people who sought to show their support of WikiLeaks.

Political hacktivism has become more common in recent years. Examples include an Anonymous cyberattack launched in Michigan to protest the water crisis in Flint. The group posted a video that accused the local media of hiding facts related to the crisis from the public, and threated action against officials who were responsible for the crisis, particularly the governor, who they claimed should be charged criminally. The hospital, the Hurley Medical Center, was also the victim of a cyberattack the day after the original attack. Another example is an attack launched against the North Carolina government website to protest a state law that would require transgender people to use the bathrooms of their sex as noted on their birth certificate. Despite the attack, the websites were not brought down and were operational, making the attack less effective.

It is important that all organizations, businesses and government agencies, be prepared for an act of hacktivism. They should ensure that their computer networks have updated security measures to block hackers from accessing their computers. They also need to develop a plan to respond to an attack if it happens. This way, the damage from an attack can be minimized.

See also: Anonymous; Assange, Julian; Denial-of-Service Attack (DoS); Hacker and Hacking; Sony Pictures Entertainment Hack; WikiLeaks

Further Reading

Bergal, Jennin. 2017. "Hacktivists launch more cyberattacks against local, state governments." PBS News Hour, January 10, 2017. https://www.pbs.org/newshour/nation/hacktivists-launch-cyberattacks-local-state-governments

Cult of the Dead Cow. cultdeadcow.com/

Jordan, T. and P. Taylor. 2004. *Hacktivism and cyber wars*. London: Routledge.

McCormick, Ty. 2013. "Anthropology of an idea: Hacktivism." *Foreign Policy*, 200 (May/June): 24–25.

Menn, Joseph. 2019. "Beto O'Rourke's secret membership in America's oldest hacking group." *Reuters*, March 15, 2019. https://www.reuters.com/investigates/special-report/usa-politics-beto-orourke/

Taylor, Paul. 2001. "Hacktivism: In search of lost ethics?" In *Crime and the internet*, edited by David S. Wall. New York: Routledge, pp. 59–73.

Vamosi, Robert. 2011. "How hacktivism affects us all." *PC World*, September 6, 2011. https://www.pcworld.com/article/239594/how_hacktivism_affects_us_all.html

HATE CRIME

A hate crime is any crime committed where the victim is targeted based on their race, ethnicity, sex, gender, sexual orientation, religion, or similar factor. In the United States, hate crimes are generally handled one of two ways: as its own offense, or as an allegation or sentence enhancement added to a crime. For example, if someone assaults the victim because the victim is gay, that person could be charged with assault, and that assault would be designated a hate crime. Hate crimes can take place on the internet. Certainly, crimes that require physical contact with the victim such as murder, rape, and assault cannot take place online. However, crimes such as threatening, intimidating, harassment, and stalking can take place via online communications.

In the United States, it is a hate crime if someone injures or attempts to injure via a weapon a victim selected because of their race, religion, national origin, gender, sexual orientation, or gender identity (18 U.S. Code § 249). Hate crimes, however, are by no means uniform across the United States. In fact, the exact definition of a hate crime does not appear to be uniform, either. By way of example, the Anti-Defamation League (2018) claims that five states (Arkansas, Georgia, Indiana, South Carolina, and Wyoming) have no hate crime laws, whereas the National Association for the Advancement of Colored People (2017) seems to indicate that four states (Georgia, Indiana, Utah, and Wyoming) lack hate crime laws, or at least hate crime laws that would increase the penalties for those offenders whose victim selection was motivated by race, gender, and so on. Among those states that do have hate crime laws, there is variance in the classes that are afforded protection under those laws. Race, ethnicity, and religion are generally protected in states that do have hate crime statutes. Most states that have a hate crime statute also cover gender, sexual orientation, and disability. Age is not as thoroughly included, though it is included in roughly a third of the states' hate crime statutes. A growing number of states cover gender identity in their hate crime statutes. Political affiliation is covered in just a few jurisdictions—California, Iowa, Louisiana, South Carolina, West Virginia, and the District of Columbia—as is homelessness—Alaska, California, Florida, Maine, Maryland, Rhode Island, Washington, and the District of Columbia (see National Association for the Advancement of Colored People, 2017; National Coalition for the Homeless, 2012).

In the United States, there were over 7,000 hate crimes committed in 2017—a jump from the year prior where over 7,000 hate crimes were committed (Federal Bureau of Investigation, 2017, 2018). The majority of those crimes involved a victim who was targeted because of their race or ethnicity. Just over 20 percent involved a victim who was targeted because of their religion, and roughly 16 percent were targeted because of their sexual orientation. The majority of these crimes were crimes against the person (e.g., murder, rape, assault, intimidation).

There is a distinction between a hate crime and hate speech. A hate crime involves criminal behavior exacted against a victim based on the victim's membership in a protected class (e.g., race, religion, gender). Hate speech is the conveying of a hateful message against people of a protected class. Hate crimes can be criminalized. Under the Free Speech Clause of the First Amendment to the U.S. Constitution, hate speech is protected and cannot be criminalized (*Matal v. Tam*, 137 S.Ct. 1744 (2017)). A hateful message directed towards a protected class is not a crime in and of itself. The communication must cross the line into speech that is not protected by the First Amendment to be a crime—such as threatening to do harm to someone because of their race.

Even though an online communication may be protected by the First Amendment, this does not mean there will not be repercussions for those who use hate speech online. The provisions in the U.S. Constitution only constrain the actions of government officials. In other words, a citizen's free speech can only be violated if a government official attempts to restrain those rights. Private entities are free to restrain speech as they see fit. Several online entities do prohibit hate speech on their websites, such as Facebook, Twitter, and Instagram (Facebook, 2018; Instagram, 2018; Twitter, 2018). Thus, while hate speech may not be a crime, using it can get a user potentially banned from using certain social media platforms, message boards, or other websites. Several well-known people have had their social media accounts suspended for this reason. YouTube star PewDiePie had his Twitter account temporarily suspended in 2016 after making a joke about ISIS—a group designated as a terrorist organization in the United States and numerous other countries—on his account (Shah, 2016). Actress Rose McGowan had her Twitter account temporarily suspended in 2017. McGowan—one of several women who has accused movie produced Harvey Weinstein of sexually assaulting them—made a string of posts about Weinstein's sexual misconduct right before she was suspended. Twitter indicated the suspension was due to the inclusion of a phone number of someone famous in one of her posts (Bowles and Buckley, 2017). Alex Jones—host of his own radio show and creator of the website Infowars—was banned from several social media platforms in 2018, including Twitter, Facebook, and YouTube. Facebook banned him for violating its hate speech policy. YouTube appeared to ban him for the same reason (Hern, 2018). Twitter banned him permanently for violating its abusive behavior policy (Conger and Nicas, 2018).

Where people enjoy a degree of anonymity online, research has found that the level of hate speech and related crimes has risen with the advent of the internet (Banks, 2010). This anonymity also makes enforcement of hate crimes in the cyber realm difficult.

See also: Cyberbullying; Doxing; Social Media; State Actor

Further Reading

Anti-Defamation League. 2018. "#50StatesAgainstHate: An initiative for stronger hate crime laws." Anti-Defamation League. https://www.adl.org/50statesagainsthate

Banks, James. 2010. "Regulating hate speech online." *International Review of Law, Computers & Technology* 24, 3: 233–239.

Bowles, Nellie, and Cara Buckley. 2017. "Rose McGowan's Twitter account locked after posts about Weinstein." *New York Times*, October 12, 2017. https://www.nytimes.com/2017/10/12/arts/rose-mcgowan-twitter-weinstein.html

Conger, Kate, and Jack Nicas. 2018. "Twitter bars Alex Jones and Infowars, citing harassing messages." *New York Times*, September 6, 2018. https://www.nytimes.com/2018/09/06/technology/twitter-alex-jones-infowars.html

Facebook. 2018. "Hate speech." https://www.facebook.com/communitystandards/hate_speech

Federal Bureau of Investigation. 2017. "Uniform crime reports: Hate crime statistics, 2016." https://ucr.fbi.gov/hate-crime/2016

Federal Bureau of Investigation. 2018. "Uniform crime reports: Hate crime statistics, 2017." https://ucr.fbi.gov/hate-crime/2017

Hern, Alex. 2018. "Facebook, Apple, YouTube and Spotify ban Infowars' Alex Jones." *The Guardian*, August 6, 2018. https://www.theguardian.com/technology/2018/aug/06/apple-removes-podcasts-infowars-alex-jones

Instagram. 2018. “Community guidelines.” https://help.instagram.com/477434105621119

National Association for the Advancement of Colored People. 2017. “State-by-state hate crime laws.” https://www.naacp.org/wp-content/uploads/2017/09/Hate-Crimes-laws-by-state.pdf

National Coalition for the Homeless. 2012. *Hate crimes against the homeless: An organizing manual for concerned citizens*. National Coalition for the Homeless. https://nationalhomeless.org/publications/hatecrimes/hatecrimesmanual12.pdf

Shah, Saqib. 2016. “PewDiePie suspended from Twitter after tweeting Islamic State joke.” *Digital Trends*, August 31, 2016. https://www.digitaltrends.com/social-media/pewdiepie-twitter-ban/

Twitter. 2018. “Hateful conduct policy.” https://help.twitter.com/en/rules-and-policies/hateful-conduct-policy

HEALTH CARE, EFFECTS ON

Cybercrime poses a growing threat to health care. In the late 2010s, cyberattacks on health care facilities and health care providers became more frequent and more serious. In 2015, cybercriminals targeted the health care industry more than any other sector (Zorabedian, 2016). One survey of the health care industry showed that 90 percent of health care groups report having suffered a data breach within the previous two years. According to the Identity Theft Resource Center, over 45 percent of computer breaches were health care related (RSA, 2011). Hacking crimes can be carried out against health care providers, health care business associates, health plans, health care clearinghouses, pharmaceuticals, and other related groups. Some estimates show that the health care industry in the United States must pay over $6 billion a year because of cyberattacks (Socas, 2015).

Breaches in health care systems compromise the personal information of millions of patients. If an offender is able to hack into another person’s medical records, the offender may be able to use the stolen information to commit many other types of crimes. Common offenses include fraud or identity theft. Identity theft becomes an attractive crime to some offenders who are seeking medical care, and can do so under another’s identity. They may choose to use a patient’s insurance information fraudulently. When this happens, patients may spend thousands of dollars to get their personal health care records cleared. In the meantime, though, a victim may not have access to medical care.

It is difficult for health care agencies to protect themselves. They often do not have the resources nor the technological skill to prevent or deter the attacks. The antivirus software that health care providers rely on is often outdated and not effective in preventing attacks.

The health care field is an attractive target for cybercriminals. Most medical records today are electronic. It is easier and safer to track records and transfer records in this form as compared to paper. This availability of online health records gives offenders more opportunities to steal or compromise files. The files hold a great deal of personal information on patients, including their birthdates (and ages), family status, place of employment, Social Security numbers, medical conditions, and sometimes even payment methods. It is reported that a stolen medical record can be sold for only $20 on the dark web, which can be more money than an offender can charge for a stolen credit card number (Wedi, 2017).

The Health Insurance Portability and Accountability Act of 1996, or HIPA, mandates that healthcare agencies have safeguards in place to protect a patient's privacy. A doctor or other health care professional who does not abide by these guidelines can face serious federal charges. If data files are accessed illegally, the organization may face fines for being out of compliance with regulations. They may also be opened to lawsuits from victims. They may also face damage to their reputation among the public.

Recent cyberattacks on health care facilities have caused serious damage. In March 2016, a cyberattack carried out on MedStar Health, a system that served clients in Maryland and Washington, D.C., infected the system with malware that caused it to lose access to patient records. The attack forced the company to shut down multiple computer systems as a preventive measure to keep the malware from spreading. Health care facilities in Kentucky, California, and Canada were victims of ransomware attacks and were forced to pay money to an attacker in order to have access to the patient's files. Hollywood Presbyterian Medical Center in California reportedly paid $17,000 in Bitcoin (about 40 Bitcoins) in a ransom payment after they were attacked (Secure 360, 2016). The hospital was forced to shut down all of their computers for a week, and instead depended on paper records.

Breaches on health care facilities can be dangerous for both the company and the victim. It is critical that companies keep their anti-virus programs updated and watch for breaches regularly as a way to prevent attacks.

See also: Bitcoin; Economy, Effects on; Personally Identifying Information; Prevention; Ransomware

Further Reading

RSA. 2011. "Cybercrime and the healthcare industry." Healthcare Info Security, September 13, 2011. http://www.healthcareinfosecurity.com/whitepapers/cybercrime-healthcare-industry-w-338

Secure 360. 2016. "The effects of cyber attacks on the health care industry." June 15, 2016. https://secure360.org/2016/06/the-effects-of-cyber-attacks-on-the-health-care-industry/

Socas, James. 2015. "Growing pains: Cybercrime plagues the healthcare industry." Healthcare IT News, December 21, 2015. http://www.healthcareitnews.com/blog/growing-ains-cybercrime-plagues-healthcare-industry.

Workgroup for Electronic Data Interchange. 2017. "The rampant growth of cybercrime in health care." February 8, 2017. www.wedi.org/docs/publications/cybercrime-issue-brief.pdf

Zorabedian, John. 2016. "Why cybercriminals attack healthcare more than any other industry." *Naked Security*, April 26, 2016. https://nakedsecurity.sophos.com/2016/04/26/why-cybercriminals-attack-healthcare-more-than-any-other-industry

HIJACKING

The term "hijacking" refers to an attack on a network in which the offender is able to take over control of a communication between a sender and recipient, or maybe the offender takes over a person's online account and uses it. The offender pretends to be the sender in the communication. In some cases, the offender is able to trick the victim into providing private information, credit card information, passwords, or other types of sensitive information. This gives the offender the ability to carry out further acts against the victim. In more serious accounts, an account can be completely erased.

One specific type of hijacking attack is called the "browser hijacking." In this case, the user is diverted to a site other than the intended site. An offender is able to modify a web browser's settings so the computer goes to sites that are not intended by the user. In other words, the software changes the activities of a browser. Most of the time, the hacker is being paid to get people to click on ads or increase the number of people who visit a web page. By hijacking other computers, the hacker can force computers to go to sites and encourage users to click on ads. Some ads will be shown on a computer numerous times. In some cases, a browser hijacker intends to install malware to enable them to steal personal information.

Another specific type of hijacking is the "man in the middle" (MIM) attack, whereby the offender controls an ongoing communication between two people. The offender is able to watch and monitor any communication as it takes place, and if they choose, they can intercept a message and replace it with their own message before it is resent. The people in the conversation have no idea their messages have been replaced. This way, it appears to the receiver that they are still communicating with the intended person. The replaced message may be an attempt to ruin a reputation, or it can be a way to trick the receiver into providing personal data to the offender.

An example of this is if a person receives an e-mail from a bank asking them to verify their account information. The e-mail appears to be from a bank employee, so the victim provides the information. In essence, the victim is giving their personal account information to an offender, who can now enter into a site and steal money.

Another form of hijacking is pharming, where malware is applied to a computer, which causes the user to land on bogus websites that appear to be the actual webpage. A victim, thinking they are on a legitimate site, may type in a password or other personal or sensitive information. This is then stolen by the hacker and sold or used to commit other cybercrimes.

There are two types of hijacking. The first is passive hijacking, where the offender hijacks a session but then simply watches the communication. This way, they remain hidden to the users. This is a technique that allows the hacker to look for passwords or other sensitive information. It is said that the hacker "sniffs" the network. The second type of hijacking is active hijacking. In an active hijacking, the offender will take over the server within the conversation. At that point, the offender can replace one of the people in the conversation or can change passwords, delete files or e-mails, create new e-mails, or download files (which could include malware).

See also: Identity Theft; Malware; Phishing

Further Reading

Cucu, Paul. 2017. "Session hijacking takes control of your accounts. Here's how." Heimdal Security, August 4, 2017. https://heimdalsecurity.com/blog/session-hijacking/

Kaspersky. "What is browser hijacking?" https://www.kaspersky.com/resource-center/threats/browser-hijacking

Pegoraro, Rob. 2004. "For Windows users, 'browser hijacking' is only the latest threat." *The Washington Post*, February 24, 2004. http://www.washingtonpost.com/wp-dyn/articles/A14264-2004Feb28.html

Techopedia. "Man-in-the-middle attack (MITM)." https://www.techopedia.com/definition/4018/man-in-the-middle-attack-mitm

I

IDENTITY THEFT

Identity theft occurs when someone obtains and uses the personally identifying information of someone without their permission. This includes someone's name, date of birth, social security number, and bank account number. It also includes someone's username and password for their e-mail and social media accounts.

Identity theft is different from basic theft. Unlike basic theft, identity theft does not require that the perpetrator wrongfully obtain property. It simply requires that the perpetrator wrongful use the identifying information of the victim with the intent to wrongfully obtain property from the victim. Thus, if someone were to take the identifying information of a victim with the intent to steal money from the victim, but was caught before they were able to use that information to steal the money, they would still be guilty of identity theft.

Identity theft can also be committed by taking the personal information of another with the intent to do harm to the victim in general. While taking money from a victim is one form of harm, identity theft does not limit the harm to financial loss. For example, someone could take the personal information of another with the intent to impermissibly log into a victim's e-mail account to find and publicly disclose information damaging to the victim, such as photos or the contents of e-mails.

Identity theft is a widespread problem. It is estimated that roughly 7 percent of people in the United States age 16 or older (over 17 million people) experience some form of identity theft annually, and that 15 percent of people will be the victim of identity theft at some point in their lives (Harrell, 2015). Less than half of those victims know how their personal information was obtained. The incidents result in billions of dollars of losses to victims annually (approximately $24 billion in 2012 and $15 billion in 2014). In addition to financial loss, victims of identity crimes often have to deal with the emotional stress of being victimized and having to spend time resolving the theft of their identity (Harrell, 2015).

Given the prevalence of identity theft, the United States government has provided tips for citizens to help prevent their identity from being stolen, including offline and online measures. Offline measures include not carrying a social security card, promptly collecting mail, and shredding documents with personal information before throwing them away, such as receipts, credit card offers, and bank statements. Online measures include not responding to unsolicited requests for personal information, using security features on electronic devices (e.g., tablets, cell phones), and the installation of antivirus software on personal computers (United States of America, 2018).

Even if someone follows the recommendations of law enforcement to protect their identity, they may still become the victim of identity theft. Data breaches at major companies have become commonplace. In 2011, Sony suffered a breach affecting 77 million customers (Baker and Finkle, 2011). In 2013, Yahoo suffered a breach affecting 3 billion customers (Larson, 2017). In 2014, eBay suffered a breach affecting 145 million customers (Wakefield, 2014). While individuals can choose to be members or users of companies like Sony, Yahoo, or eBay, the 2017 breach of Equifax showed that some companies possess citizens' personal information without them being aware of it. As a credit reporting agency, Equifax is able to legally obtain the credit information of individuals to construct a credit history for those individuals as well as generate a credit score. This information is then provided to businesses when you attempt to engage in certain transactions with them, such as applying for a new credit card, renting an apartment, or seeking a car loan. In short, essentially everyone's information is likely to be in the possession of credit reporting agencies such as Equifax. Initially, Equifax estimated that 143 million people may have been affected by the data breach (Regnier and Woolley, 2017). Equifax estimates that 2.4 million additional people had their personal information stolen above their initial estimates (Equifax, 2018; Kennedy, 2018).

See also: Equifax Breach; Social Media; Sony Pictures Entertainment Hack

Further Reading

Baker, Liana B., and Jim Finkle. 2011. "Sony PlayStation suffers massive data breach." *Reuters*, April 26, 2011. https://www.reuters.com/article/us-sony-stoldendata/sony-playstation-suffers-massive-data-breach-idUSTRE73P6WB20110427

Equifax. 2018. "Announcement: What you need to know." Equifax, March 1, 2018. https://www.equifaxsecurity2017.com/

Harrell, Erika. 2015 (2017). *Victims of identity theft, 2014*. Washington, D.C.: Bureau of Justice Statistics.

Kennedy, Merit. 2018. "Equifax says 2.4 million more people were impacted by huge 2017 breach." National Public Radio, March 1, 2018. https://www.npr.org/sections/thetwo-way/2018/03/01/589854759/equifax-says-2-4-million-more-people-were-impacted-by-huge-2017-breach

Larson, Selena. 2017. "Every single Yahoo account was hacked—3 billion in all." CNN, October 4, 2017. https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html

Regnier, Pat, and Suzanne Woolley. 2017. "Thank you for calling Equifax. Your business is not important to us." *Bloomberg*, September 14, 2018. https://www.bloomberg.com/news/features/2017-09-14/thank-you-for-calling-equifax-your-business-is-not-important-to-us

United States of America. 2018. "Identity theft." United States of America. https://www.usa.gov/identity-theft#item-206114

Wakefield, Jane. 2014. "eBay faces investigations over massive data breach." *BBC*, May 23, 2014. https://www.bbc.com/news/technology-27539799

ILOVEYOU VIRUS

The ILOVEYOU virus, otherwise known as the Love Letter virus or the Love Bug, became one of the most damaging malware to be introduced—and also the most widely recognized malware. It was originally launched in May 2000, a year after the Happy99 virus spread through e-mail. The ILOVEYOU virus attacked an estimated 45 million users around the world who were using Microsoft Windows or Microsoft Outlook. Victims received an e-mail with "ILOVEYOU" written in the subject line. If a user opened the e-mail, the body of the e-mail would say, "Kindly check the attached loveletter coming from me." There was an attachment to the e-mail that contained the virus. When it was opened, the virus was activated and instantly loaded onto the victim's hard drive, where it erased photos, music, and other files. The virus then resent itself to the e-mail contacts in the victim's address book. Because a person received the e-mail from a friend or family member, they were more likely to open it.

Because the virus sent itself to all of the e-mails in the address book, it spread more quickly than other malware. If a large organization received the virus, it caused thousands of e-mails to be sent to a server. A single employee's e-mail address may be copied numerous times. Many networks were overloaded, causing slowdowns and eventually bringing down the internet. Ford Motor Company was one company that fell victim to the virus, causing their e-mail to be unavailable for a short time. Other organizations that were forced to shut down after becoming infected included the U.S. Pentagon and Britain's Parliament. It is estimated that the virus caused $10 billion in damages to companies around the world. The virus was also blamed for causing personal pagers to malfunction.

In the days after the ILOVEYOU virus swept around the world, copycat attack viruses soon appeared. One of those was named "very funny." This new virus, and others that appeared, were not detected by most virus protection software, especially software that was designed to block the ILOVEYOU virus. In some cases, the message in the subject line was changed to read "Joke," "Mother's Day," or even "Virus Alert!!!," all of which made the recipient less likely to be cautious of the contents. The new viruses were also feared to cause similar or worse damage than the original virus.

In response to the virus, the U.S. president at the time, Bill Clinton, asked that the FBI investigate the crime. The FBI assigned the task to New York's field office, with help from the offices in Newark, New Jersey, and Charlotte, North Carolina. The National Infrastructure Protection Center oversaw the investigation. It was discovered that the virus began infecting systems in Hong Kong, followed by Europe and then the U.S. law enforcement soon traced the virus to two men in the Philippines: Reonel Ramones and Onel de Guzman. Both men had dropped out of a computer university in Manilla. De Guzman had actually proposed the virus in a paper he had written for one of his courses.

Because the Philippines had no law against hacking crimes at the time, law enforcement was unable to arrest them, and the offenders were not charged with any crime.

As expected, there were many calls for backing up systems and installing updated virus protection software after the virus was detected. When the virus was launched, many personal computer users did not have virus protection, and many businesses were also lacking antivirus software. The virus made both people and organizations aware of the need for additional and updated virus protection.

See also: Federal Bureau of Investigation; Malware; Melissa Worm; President and Cybercrime

Further Reading

Goldenberg, Stuart. 2000. "Back up to beat the bug." *New York Times*, May 11, 2000. https://www.nytimes.com/2000/05/11/technology/back-up-to-beat-the-bug.html

Hill, Joshua B. and Nancy E. Marion. 2016. *Introduction to cybercrime: Computer crimes, laws, and policing in the 21st century.* Santa Barbara, CA: ABC-CLIO.

Kleinbard, David and Richard Richtmyer. 2000. "Quickly spreading virus disables multimedia files, spawns copycats." CNN Money, May 5, 2000. https://money.cnn.com/2000/05/05/technology/loveyou/

Schwartz, John, and David A. Vise. 2000. "'Love' virus assaults world computers." *Washington Post*, May 5, 2000. https://www.washingtonpost.com/archive/politics/2000/05/05/love-virus-assaults-world-computers/3079f34d-f8d9-4004-b858-7015a4e22896/

Ward, Mark. 2010. "A decade on from the ILOVEYOU bug." BBC News, May 4, 2010. https://www.bbc.com/news/10095957

IMMIGRATION AND CUSTOMS ENFORCEMENT

The Bureau of Immigration and Customs Enforcement (ICE) is a federal agency in the United States. It was created March 1, 2003, as part of a large federal government restructuring. Following the terrorist attacks of September 11, 2001, the United States formed the DHS to help protect the United States from future terrorist attacks and to help assure the safety of the country in general (Department of Homeland Security, 2015b). As part of this restructuring, the DHS absorbed all or part of 22 federal agencies and programs. Two of those were the Immigration and Naturalization Service and the Customs Service. These responsibilities of these two agencies were parsed out to three separate agencies under the Department of Homeland Security: the Bureau of Customs and Border Protection, the Bureau of Citizenship and Immigration Services, and the Bureau of Immigration and Customs Enforcement (Bureau of Immigration and Customs Enforcement, 2019). The mission of ICE is to "protect America from the cross-border crime and illegal immigration that threaten national security and public safety" (Bureau of Immigration and Customs Enforcement, 2018). Cybercrimes that take place in a cross-border fashion are investigated by the bureau's Cyber Crime Center. The Center was created in 1997 under the control of the U.S. Customs Service, but it was placed under the authority of ICE following the absorption of the U.S. Customs Service into the Department of Homeland Security (Department of Homeland Security, 2015b).

Among the cybercrimes that ICE investigates are child exploitation cases. In 2009, ICE launched Operation Delego—an investigation into a pedophilia-promoting website called Dreamboard. Members of the site lived in numerous countries. In order to be a member of the site, a prospective member had to upload child pornography involving children 12 years old or younger. To maintain membership, members had to continually upload child pornography to the site. The more child pornography a member uploaded, the more they would be able to access from the site's archive. Members who uploaded child pornography with themselves perpetrating the sex acts on children gained even greater access to the site's archive of child pornography. By August 2011, 72 members were charged with crimes arising from their involvement with Dreamboard, 56 of whom were arrested by that time, with 13 of those 56 having pleaded guilty to their charges (Holder, 2011).

Additionally, as part of their cybercrime unit, ICE operates a child victim identification program. The first case the program assisted with was in November 2011. In that case, an 11-year-old girl's picture showed up on a website known to be frequented by pedophiles. There was a poll along with her picture, asking members of the website how this girl should be raped. Danish law enforcement first noticed the picture and poll and contacted ICE. Agents with ICE were able to use the girl's picture—specifically, a street sign in the background with a sunflower on it—to locate her in Kansas (where state highway signs have sunflowers on them) and rescue her (see Department of Homeland Security, 2018). In November 2012—a year after this girl was rescued—ICE initiated Operation Sunflower. The goal of this operation was to rescue child victims of sexual exploitation and to apprehend those exploiting them. The operation lasted roughly a month. In that time, ICE was able to identify 123 child victims, 44 of whom were rescued. The remaining 79 children were either abused by someone outside of the home they lived in or were adults at the time ICE contacted them (Bureau of Immigration and Customs Enforcement, 2013a).

ICE has been involved in cybercrime cases not involving child sexual exploitation as well. In 2013, it was involved in Operation Marco Polo—an investigation of the dark web marketplace Silk Road. The site was used to facilitate the sale of illegal drugs and other criminal contraband. As a result of the investigation, Silk Road was shut down, and its creator—Ross Ulbricht (also known as Dread Pirate Roberts)—was arrested and sentenced to life in prison (Segall, 2015).

The Cyber Crime Center was impersonated as part of malware that made its rounds in 2013. Victims' computers displayed a message that claimed to be from the Cyber Crime Center. The message told victims that their computer had been frozen due to the victim engaging in illegal activity online. The malware did in fact lock victims out of their computers. The message went on to tell victims that they needed to pay a several-hundred-dollar fee to avoid prosecution. It further threatened that if victims attempted to unlock their computers, all files on the computer would be deleted (Pilici, 2013). ICE notified the public of this hoax in February 2013 (Bureau of Immigration and Customs Enforcement, 2013b).

See also: Child Pornography; Dread Pirate Roberts (Ulbricht, Ross; 1984–); Federal Bureau of Investigation; Operation Marco Polo; Silk Road

Further Reading

Bureau of Immigration and Customs Enforcement. 2013a. "123 sexually exploited children identified by HSI during 'Operation Sunflower.'" Bureau of Immigration and Customs Enforcement, January 3, 2013. https://www.ice.gov/news/releases/123-sexually-exploited-children-identified-hsi-during-operation-sunflower

Bureau of Immigration and Customs Enforcement. 2013b. "SCAM ALERT: Cyber criminals masquerade as the ICE Cyber Crimes Center to extort money from web users." February 15, 2013. https://www.ice.gov/news/releases/scam-alert-cyber-criminals-masquerade-ice-cyber-crimes-center-extort-money-web-users

Bureau of Immigration and Customs Enforcement. 2018. "What we do." https://www.ice.gov/overview

Bureau of Immigration and Customs Enforcement. 2019. "Celebrating the history of ICE." Bureau of Immigration and Customs Enforcement. https://www.ice.gov/features/history

Department of Homeland Security. 2015a. "DHS unveils major expansion of ICE Cyber Crimes Center." Department of Homeland Security, July 22, 2015. https://www.dhs.gov/news/2015/07/22/dhs-unveils-major-expansion-ice-cyber-crimes-center

Department of Homeland Security. 2015b. "Creation of the Department of Homeland Security." September 24, 2015. https://www.dhs.gov/creation-department-homeland-security

Department of Homeland Security. 2018. "Cyber crime cases." Retrieved from https://www.dhs.gov/cyber-crime-cases on October 19, 2018.

Holder, Eric. 2011. "Attorney General Eric Holder announces results of international child pornography investigation at Operation Delego press conference." United States Department of Justice, August 3, 2011. https://www.justice.gov/opa/speech/attorney-general-eric-holder-announces-results-international-child-pornography

Pilici, Stelian. 2013. "The ICE Cyber Crime Center—Virus removal guide." Malwaretips.com, June 12, 2013. https://malwaretips.com/blogs/ice-cyber-crime-center-removal/

Segall, Laurie. 2015. "Silk Road's Ross Ulbricht sentenced to life." CNN, May 29, 2015. https://money.cnn.com/2015/05/29/technology/silk-road-ross-ulbricht-prison-sentence/index.html

INSURANCE

Cybersecurity insurance or cyber risk insurance has become a popular way for companies, organizations, and individuals to protect their agencies or themselves against damages that can result from a cyberattack and, for some, to help them survive the aftermath of an attack. Cyber insurance first became available in the mid-1990s as the internet became more widely used. In the beginning, the insurance plans were made available by a limited number of companies for a limited amount of protection. The number of organizations and individuals opting to purchase insurance has increased since then. Today, the cyber insurance industry is rapidly expanding and has become part of many organizations' incident response plans as they prepare for the inevitable attack. It is often purchased not only by those in the health care or banking industries but also by those in retail, education, manufacturing, and transportation.

Cyber insurance is the result of the increased number of cyberhacks that occur each year. Not only are there more frequent attacks, but they are also becoming more serious and more damaging. Companies are purchasing insurance as a way to minimize the costs of an attack, which can be thousands of dollars, rising into the millions for a large hack on a large corporation. Cyber insurance is especially critical for small or midsize companies that may have less security than larger firms and may be more vulnerable to an incident. A cyberattack on a small company could be devastating. Unfortunately, many smaller companies are choosing to forgo insurance. Recent statistics show that about 55 percent of Fortune 500 companies have purchased some form of cyber insurance. That percent drops to 35 percent for medium-sized businesses and only 10 percent for small businesses (Fazzini, 2018). In all, companies spent over $2 billion on cyber insurance in 2017 (Fazzini, 2018). This number could rise to $20 billion by 2025 (Sloan, 2017).

Cyber insurance premiums vary and cover different costs related to a computer hacking event. Some insurance plans assist a company or organization to pay for recollection or recovery costs related to stolen or damaged information during a hack. Many policies will pay for access to forensic investigations to determine, if possible, the source of the attack and the techniques used for gaining access to a network. This often includes longer-term monitoring of the computer systems for months after an attack to ensure that there were no hidden backdoors or vulnerabilities placed into a system that would allow an attacker to access the systems at a later date. Insurance may also cover any legal liabilities, fines, and fees associated with a breach. Notification of all customers who may be affected by a hacking and other costs related to a settlement agreement (i.e., free credit monitoring) may be very expensive and is often included in an insurance premium. Other costs that may be covered include payments for extortion or ransomware to release data that has been locked by cybercriminals. Finally, some policies provide incident response teams to help an organization return to normal.

There are costs of an attack that are typically not covered by cyber insurance. Most policies typically do not cover the value of the loss of intellectual property or trade secrets. It is often very difficult to place a monetary value on a company's intellectual property so this is left uncovered. Most policies also do not cover any security failures that were considered to be "preventable," such as a failure of a company to maintain an acceptable or minimal level of security needed to protect the company's systems. In other words, if an organization does not have adequate cybersecurity software in place based on their level of risk, an insurance company may not cover the costs of the breach. Additionally, if company employees do not follow established protocols for ensuring the safety of data, the costs may not be covered. For example, if an employee accesses sensitive data through an unsafe network such as an airport or cybercafé, the damages may not be covered. The same holds true of an employee who carries out an "insider" attack on the company that results in a loss of data or secrets.

Companies seeking to purchase cyber insurance must find an insurance plan to fit the specific needs of the individual company. Since cyberattacks and resulting damages are unpredictable, it is difficult for companies to know exactly what kind of insurance policy to purchase. This is made more difficult because the cyber insurance industry is relatively new and coverage provided is not standard. Company officials must base their policies on the company's risk. They must determine their vulnerabilities and threats, and develop a policy to cover those. The National Institute of Standards and Technology, located within the U.S. Commerce Department, has developed security guidelines to help company officials assess their risks. The price they will pay will depend on the company's risk. A business with a higher risk of becoming the target of cybercrime will need higher or more complex coverage. The cost may also depend on the type and extent of cybersecurity put in place by an organization, any prior claims made by the company, or even the company's annual revenue. An insurance policy can cost a small company a few thousand dollars, whereas a larger organization will pay up to hundreds of thousands of dollars for full protection.

Cyber insurance is not only important to companies and organizations; individuals may purchase cyber insurance as a way to cover costs associated with identity theft, credit card theft or online fraud, or even malware attacks on a personal device or home computer. Some insurance policies will cover the legal fees associated with comments posted on social media sites that may be damaging to an individual.

There are two types of cyber insurance coverage: first-party and third-party coverage. In a first-party coverage plan, insurance covers the damages or losses that occur to individuals or businesses caused directly by a breach, such as data recovery, or compensating a business for any income that it loses (sometimes called Business Interruption Insurance), or paying a cyberextortionist who threatens to carry out an attack or uses ransomware to demand payment for the return of data. This also includes the investigation to determine how the attack occurred, notification of customers who were affected, and efforts taken to mitigate damage to a company's reputation.

Third-party insurance coverage includes damages pertaining to customers or partners who are affected. This includes the individuals and businesses responsible for a computer system that is attacked and breached. It could cover protection for an IT company that was responsible for storing data that was breached if the IT company did not anticipate an attack and take precautions, or a company that was supposed to build a secure website for a client and did not. Third-party insurance would cover any legal fees, settlements that are agreed to, or fines that may result.

See also: Ashley Madison Breach; Cybersecurity; Equifax Breach; Hacker and Hacking; National Institute of Standards and Technology Cybersecurity Framework; Ransomware

Further Reading

Bhattarai, Abha. 2014. "Cyber-insurance becomes popular among smaller, mid-size businesses." *Washington Post*, October 12, 2014. https://www.washingtonpost.com/business/capitalbusiness/cyber-insurance-becomes-popular-among-smaller-mid-size-businesses/2014/10/11/257e0d28-4e48-11e4-aa5e-7153e466a02d_story.html

Fazzini, Kate. 2018. "Cyber insurance: Companies must weigh uncertainties in an unproven market." *Wall Street Journal*, May 18, 2018. https://www.wsj.com/articles/cyber-insurance-companies-must-weigh-uncertainties-in-an-unproven-market-1525987315

Grzadkowska, Alicja. 2018. "How cybercrime and coverage evolved in 2018." *Insurance Business*, December 12, 2018. https://www.insurancebusinessmag.com/us/news/cyber/how-cybercrime-and-coverage-evolved-in-2018-118721.aspx

NTT Security. 2018. "Cybercrime insurance. A growing market. Are you covered?" https://www.nttsecurity.com/docs/librariesprovider3/resources/gbl_thought_leadership_cyber_insurance_uea.pdf?sfvrsn=90cf809d_4

Shetty, Mayur. 2017. "In a first, cybercrime insurance cover for individuals." *The Economic Times*, November 3, 2017. https://economictimes.indiatimes.com/tech/internet/in-a-first-cybercrime-insurance-cover-for-individuals/articleshow/61476025.cm

Sloan, Rob. 2017. "Cyber insurance may affect incident response industry." *Linkedin*, January 17, 2017. https://www.linkedin.com/pulse/cyber-insurance-may-affect-incident-response-industry-rob-sloan

INTERNATIONAL ISSUES

Cybercrime is unique in that the perpetrator of such a crime can be anywhere in the world where the internet is accessible, and the same applies to the victim. Accordingly, to fully and effectively fight cybercrime, international cooperation appears to be necessary. This sentiment was expressed by Meng Hongwei, former president of Interpol, in 2016. He said:

> Despite differences among countries, combating crimes and guarding the law is what police do as their nature prescribes. Professionalism and integrity is what made us friends who fought crimes side by side, and even more so in today's integrated and hi-tech world. The crimes we see are no longer those that a country can solve alone. Any crack on the globe may become a source of evil that can plague the world. Therefore it is imperative that police help each other, because it's helping ourselves. (Meng, 2017)

Meng also noted the importance of all stakeholders, not just governments, working together to fight cybercrime. It seems that many countries and other stakeholders agree. In 2018, 50 countries vowed to work together to fight cybercrime and other malicious online activity. Over 150 tech companies agreed to do the same. This commitment was memorialized in the "Paris call for trust and security in cyberspace." The countries involved include France, Japan, and Canada. The companies involved include Google, Microsoft, and Facebook. Just as notable as the entities agreeing to this combined effort are those countries that did not agree: the United States, Russia, and China (Corbet, 2018). One of the reasons there may be a lack of international cooperation to fight cybercrime is that individual countries may benefit from cybercrime that is committed within its borders. Indeed, China and Russia are the two most prolific perpetrators of cyberattacks against other countries (Center for Strategic and International Studies, 2019).

In China, the People's Liberation Army (PLA)—the Chinese military—is responsible for carrying out various cyberattacks on foreign countries and other entities. In one incident, the PLA covertly installed microchips on server motherboards manufactured in China. This allowed the PLA to scan activity on those servers, which were used by foreign government agencies and businesses (Robertson and

Riley, 2018). As part of the government, the PLA's actions are directed by the Chinese government and permit the government to engage in espionage. This cybercrime clearly benefits China, and there would be no reason it would want to help eradicate it. Chinese citizens who do not work for the government also engage in cybercrime that appears to benefit China. This includes intellectual property theft that permits Chinese industries to advance the state of technology in China (Commission on the Theft of American Intellectual Property, 2017).

Russia has acted similarly. In 2016, Russia's Main Intelligence Directorate of the General Staff (GRU) hacked into computer networks of entities associated with the campaign of presidential candidate Hilary Clinton and released information obtained from those entities with the intent of influencing the presidential election (Mueller, 2019). There is also evidence to suggest that cybercriminals in Russia that do not attack domestic targets are permitted to continue in their activities without apprehension (Maurer, 2018).

The United States has also engaged in cyberattacks on other countries. In 2010, it is believed the United States worked with Israel to bring down Iran's Natanz nuclear facility via the Stuxnet computer worm. The worm caused the computers at the nuclear facility to spin centrifuges faster than they were supposed to, damaging the centrifuges in the process (Warrick, 2011). In 2013, it is believed that the United States, in conjunction with South Korea, brought down North Korean websites and restricted internet access within the country (Center for Strategic and International Studies, 2019; Sang-Hun, 2013).

Where cyberattacks are being used by countries against each other, there does arise a question as to whether these activities are truly crimes or acts of war (Flatow, 2011; Stoll, 2018). Thus far, it appears the United States has treated such as attacks as the former. Twelve Russian officers who interfered in the 2016 presidential election in the United States were indicted on federal criminal charges (Prokop, 2019). The United States indicted five members of the PLA involved in espionage and theft against U.S. businesses (United States Department of Justice, 2014). It also indicted one member of the North Korean–sponsored Lazarus Group for his role in the hack of Sony Pictures (United States Department of Justice, 2018). The indictments appear largely symbolic, as those indicted appear to still be living in the countries that sponsored the attacks and are thus at no real risk of being extradited to the United States.

Lack of international cooperation in the extradition of cybercriminals exists beyond those incidents where the person indicted carried out cyberattacks at the behest of the country protecting them. A notable example of this is Julian Assange. Assange was being investigated in the United States for possible criminal charges arising out of his role with WikiLeaks (Weiss, 2010). Assange was granted asylum at the Ecuadorian Embassy in London in 2012 after skipping bail in the United Kingdom on an extradition matter with Sweden (BBC News, 2018). It became apparent that the United States had indicted Assange in 2018, and Ecuador protected Assange until 2019. Another notable example is Edward Snowden. After Snowden leaking NSA documents to the public, he fled to Hong Kong. While he was there, a request was made by the United States to have Snowden extradited. Hong Kong, claiming a mistake in the extradition paperwork regarding Snowden's name, delayed processing the extradition, which permitted Snowden the opportunity to leave Hong Kong for Russia (see Burrough and Ellison, 2014). Snowden has not been extradited from Russia since arriving there in 2013. He has a resident permit there that is good through 2020 (Kramer, 2017).

See also: Assange, Julian; China; North Korea; People's Liberation Army Unit 61398; Political Uses; Russia; U.S. Presidential Election Interference, 2016; WikiLeaks

Further Reading

BBC News. 2018. "Julian Assange in the Ecuadorian embassy: Timeline." BBC News, October 19, 2018. https://www.bbc.com/news/world-europe-11949341

Burrough, Bryan, and Sarah Ellison. 2014. "The Snowden saga: A shadowland of secrets and light." *Vanity Fair*, April 23, 2014. https://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview

Center for Strategic and International Studies. 2019. "Significant cyber incidents." https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

Commission on the Theft of American Intellectual Property. 2017. "Update to the IP Commission Report." http://ipcommission.org/report/IP_Commission_Report_ Update_2017.pdf

Corbet, Sylvie. 2018. "50 countries vow to fight cybercrime—US and Russia don't." *Associated Press*, November 12, 2018. https://www.apnews.com/76ea0daee12645f0ae7177eb506935cb

Flatow, Ira. 2011. "Cyberattacks may be 'acts of war.'" National Public Radio, June 3, 2011. https://www.npr.org/2011/06/03/136925541/cyber-attacks-may-be-acts-of-war

Kramer, Andrew E. 2017. "Russia extends Edward Snowden's asylum." *New York Times*, January 18, 2017. https://www.nytimes.com/2017/01/18/world/europe/edward-snowden-asylum-russia.html

Maurer, Tim. 2018. "Why the Russian government turns a blind eye to cybercriminals." *Slate*, February 2, 2018. https://slate.com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals.html

Meng Hongwei. 2017. "To ride the tide of the times and keep the hopes of a century: An Interpol that faces the future." Interpol, September 26, 2017. https://www.interpol.int/content/download/5351/file/Speech%20by%20President%20Meng%20Hongwei%2086GA.pdf

Mueller, Robert S. 2019. "Report on the investigation into Russian interference in the 2016 presidential election." Volume 1. United States Department of Justice. https://www.justice.gov/storage/report.pdf

Prokop, Andrew. 2019. "All of Robert Mueller's indictments and plea deals in the Russia investigation." *Vox*, March 22, 2019. https://www.vox.com/policy-and-politics/2018/2/20/17031772/mueller-indictments-grand-jury

Robertson, Jordan, and Michael Riley. 2018. "The big hack: How China used a tiny chip to infiltrate U.S. companies." *Bloomberg Businessweek*, October 4, 2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Sang-Hun, Choe. 2013. "North Korea sees South and U.S. behind cyberstrikes." *New York Times*, March 15, 2013. https://www.nytimes.com/2013/03/16/world/asia/north-korea-sees-south-us-behind-cyberstrikes.html

Stoll, Richard J. 2018. "Is a cyberattack an act of war?" *Houston Chronicle*, July 26, 2018. https://www.houstonchronicle.com/local/gray-matters/article/russia-cyberattacks-act-of-war-military-force-13107824.php

United States Department of Justice. 2014. "U.S. charges five Chinese military hackers for cyber espionage against U.S. corporations and a labor organization for commercial advantage." May 19, 2014. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

United States Department of Justice. 2018. "North Korean regime-backed programmer charged with conspiracy to conduct multiple cyber attacks and intrusions." September 6, 2018. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

Warrick, Joby. 2011. "Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack." *Washington Post*, February 16, 2011. http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html

Weiss, Baruch. 2010. "Why prosecuting WikiLeaks' Julian Assange won't be easy." *Washington Post*, December 5, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/12/03/AR2010120303267.html

INTERPOL

Interpol, whose full name is the International Criminal Police Organization, is a law enforcement organization that spans 194 countries. Its headquarters are in Lyon, France. Interpol provides various services for law enforcement around the world. This includes the maintenance of numerous databases on crimes and criminals that are available for law enforcement to access in member countries, investigative support, and training (Interpol, 2019a). Cybercrimes are among the crimes for which these services are provided.

Interpol was founded in September 1923. It was initially headquartered in Vienna, Austria, and was called the International Criminal Police Commission. During World War II, the Nazis took control of the organization, leading most countries to discontinue their participation in the organization. After falling under Nazi control, the organization was moved to Berlin, Germany. Following World War II, the organization was rebuilt in 1946, with its new headquarters in Paris, France. At that time, the organization adopted "INTERPOL" as its telegraph address—the moniker by which the organization now goes by. Its headquarters moved to Saint Cloud, France, in 1966 and then again to its current location in Lyon, France, in 1989 (Interpol, 2019b). In April 2015, Interpol opened its Global Complex for Innovation in Singapore. Within the complex is housed the Digital Crime Centre—a center for providing assistance on international cybercrimes. While this center did not open until 2015, Interpol was involved in the investigation of cybercrimes prior to this (Interpol, 2015).

Interpol has focused on working with both the public and private sector in addressing cybercrime. Interpol (in cooperation with Europol) has hosted a cybercrime conference since 2013 which focuses on the ways the public and private sector can work together. Said Tim Morris, Interpol's Executive Director of Police Services, "Only through a concerted globalized effort which maximizes our expertise and minimizes the gaps will we be best prepared to tackle emerging cyberthreats" (Interpol, 2018). This can be seen in several of their cybercrime investigations. In 2015, Interpol worked with four organizations in the private sector (Cyber Defense Institute, Kaspersky Labs, Microsoft and Trend Micro) to take down the Simda botnet (Interpol, 2015). In 2017, Interpol worked with eight countries (China, Indonesia, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam) and seven organizations in the private sector (Booz Allen Hamilton, British Telecom, Cyber Defense Institute, Fortinet, Kaspersky Lab, Palo Alto Networks, and Trend Micro) to provide analysis of cybercrime threats in seven of the eight participating countries (all but China). In regards to this operation, Noboru Nakatani—Interpol's Executive Director at the time—said that "[s]haring intelligence was the basis of the success of this operation, and such cooperation is vital for long term effectiveness in managing cooperation networks for both future operations and day to day activity in combating cybercrime" (Interpol, 2017).

See also: Bots and Botnets; International Issues

Further Reading

Interpol. 2015. "INTERPOL coordinates global operation to take down Simda botnet." April 13, 2015. https://www.interpol.int/en/News-and-Events/News/2015/INTERPOL-coordinates-global-operation-to-take-down-Simda-botnet

Interpol. 2017. "INTERPOL-led cybercrime operation across ASEAN unites public and private sectors." April 24, 2017. https://www.interpol.int/en/News-and-Events/News/2017/INTERPOL-led-cybercrime-operation-across-ASEAN-unites-public-and-private-sectors

Interpol. 2018. "INTERPOL-Europol conference calls for global response to cybercrime." September 18, 2018. https://www.interpol.int/en/News-and-Events/News/2018/INTERPOL-Europol-conference-calls-for-global-response-to-cybercrime

Interpol. 2019a. "What is INTERPOL?" https://www.interpol.int/en/Who-we-are/What-is-INTERPOL

Interpol. 2019b. "Key dates." https://www.interpol.int/en/Who-we-are/Our-history/Key-dates

K

KEYSTROKE MONITORING

Keystroke monitoring is where the keystrokes made by someone on a keyboard or other electronic device are captured and logged. Cybercriminals can use keystroke monitoring to capture the personally identifying information of victims (credit card information, login credentials, social security number, etc.) when it is typed in on the victim's computer or other electronic device. This information can then be used to defraud the victims.

Keystroke monitoring is not per se illegal. There are legitimate uses for it. Permissible monitoring activities can include a parent monitoring the activities of a child, an employer monitoring the activities of employees, or law enforcement monitoring the activities of suspected criminals (McAfee, 2013). In these instances, there may be requirements to be met to assure the monitoring is legal. Generally, it appears that the person being monitored may need to be made aware of it. This appears to have been a factor in the federal case of *Rene v. G.F. Fishers, Inc.*, 817 F. Supp. 2d 1090 (2011). In that case, Lisa Rene worked for G. F. Fishers Inc. Fishers had installed keystroke monitoring software on the computer located at the store Rene worked at. Rene was not made aware of the presence of the keystroke monitoring software. She accessed her bank account and personal e-mail account through this computer. Those accounts were then accessed by other employees at Fishers that had access to the information gathered by the keystroke monitor. The court allowed Rene's complaint to proceed against Fishers under the federal Stored Communications Act and Indiana Wiretap Act. For law enforcement, making a suspect aware of the fact that they are being monitored defeats the purpose of monitoring that suspect in the first place. In those instances, law enforcement would need to obtain a warrant to conduct the monitoring. An example of this can be seen in the federal case of *United States v. Scarfo*, 180 F. Supp. 2d 572 (2001). In that case, FBI agents obtained a search warrant and searched the business of Nicodemo Scarfo and Frank Paolercio for evidence of illegal gambling and loansharking that they were believed to be involved in. When searching a computer at the business, they came across an encrypted file they were unable to access. Believing that file held evidence of the crimes Scarfo and Paolercio were suspected of, FBI agents obtained a separate warrant to install a keystroke monitor on the computer to surreptitiously capture the password to get into that file. They were ultimately able to accomplish this through use of the keystroke monitor, and found incriminating evidence in the encrypted file.

There are some uses for keystroke monitors outside of detecting potential wrongdoing. For example, keystroke monitors have been used in research on how people write (Chan, 2017; Leijten and Van Waes, 2013).

Keystroke monitors can be used alone by cybercriminals, or in conjunction with other malware. A possible paring would be the use of a logic bomb with a keystroke monitor. A logic bomb is malware that is triggered upon the occurrence of some event. When paired with a logic bomb, a keystroke monitor can be set up to operate only after specific websites (bank websites, e-mail websites, etc.) have been visited on a compromised computer (Armendariz, 2019). This limits the amount of text a keystroke monitor captures, which in turn limits the amount of keystrokes in a log that a cybercriminal will have to sift through to discover personally identifying information of the victim.

Keystroke monitors can simply be software, or it can be hardware with software installed on it. When it is just software, a keystroke monitor can be disseminated any of the ways malware in general is disseminated (McAfee, 2013). There are different types of hardware that exist when looking at physical keystroke monitors. Some are small universal serial bus (USB) devices that can be placed on the USB connection of a USB keyboard before it is plugged into the USB port of a computer. Others are keypad plates that go over an existing keypad. These tend to be used at ATM machines and other terminals where monetary transactions take place. The keypad plate is designed to fit over the existing keypad on an ATM machine, and it appears to be the actual keypad. The device is also designed to trigger the buttons underneath them, thus allowing a victim to complete a financial transaction by putting in their PIN number, being none the wiser that their PIN number has been stolen. These are often used with skimmers—physical devices that fit over payment card slots on ATM machines and similar terminals. Using a skimmer with a keypad-style keystroke monitor allows cybercriminals to obtain both the payment card information and the associated PIN number from a victim (Federal Deposit Insurance Corporation, 2018).

There are measures that can be taken to avoid falling victim to keystroke monitoring. As when trying to avoid malware in general, it is best to avoid suspicious websites and avoid downloading suspicious files, whether on a website or on an attachment in an e-mail. Additionally, to circumvent the harms posed by keystroke monitors, password managers and onetime passwords can be used. A password manager will automatically enter login credentials for a user, thus removing the need to type in a username and password and depriving a keystroke monitor of the opportunity to capture those keystrokes. Onetime passwords, as the name indicates, can only be used once. Each time a user logs into an account that employs onetime passwords, a new password will have to be used. Thus, even if a cybercriminal is able to capture a onetime password via a keystroke monitor, that password will be invalid on a subsequent login attempt. There are other methods that can be used, such as the use of a keyboard with a non-QWERTY key layout. These can work, as most keystroke monitors will be based on the standard QWERY layout, and the use of an alternate layout will cause the keystroke log generated for a cybercriminal to be inaccurate. However, these can be inconvenient, as many people may not be accustomed to alternate key layouts for general use. Also, it is possible that cybercriminals may be aware of common alternative layouts and would be able to convert the keystrokes to a readable format (McAfee, 2013).

See also: Federal Bureau of Investigation; Identity Theft; Logic Bomb; Password; Personally Identifying Information; Skimmer

Further Reading

Armendariz, Tommy. 2019. “What is a logic bomb?” Lifewire, March 4, 2019. https://www.lifewire.com/what-is-a-logic-bomb-153072

Chan, Sathena. 2017. “Using keystroke logging to understand writers’ processes on a reading-into-writing test.” *Language Testing in Asia* Vol. 7, No. 10. https://doi.org/10.1186/s40468-017-0040-5

Federal Deposit Insurance Corporation. 2018. “Beware of ATM, debit and credit card ‘skimming’ schemes.” https://www.fdic.gov/consumers/consumer/news/cnwin18/cardskimming.html

Leijten, Marielle, and Luuk Van Waes. 2013. “Keystroke logging in writing research: Using inputlog to analyze and visualize writing processes.” *Written Communication* 30, 3: 358–392.

McAfee. 2013. “What is a keylogger?” McAfee, June 23, 2013. https://securingtomorrow.mcafee.com/consumer/family-safety/what-is-a-keylogger/

L

LEGION OF DOOM

Legion of Doom, or LOD, is a 15–20 member computer hacker group that was based in the United States. Vincent Louis Gelormine, otherwise known as Lex Luthor (based on the character in DC Comics), founded the group in 1984 after he had a disagreement with his previous hacking group, Knights of Shadow. Known at the time for being one of the most prominent hacking groups among hackers, the group sought to infiltrate telephone networks that connected government computer systems with corporate systems.

The members of the group were hackers who sought to exchange information about their unauthorized hacking experiences as well as hacking techniques and methods. Many of their tips were published in the *Legion of Doom Technical Journal* that provided information of interest to other hackers, such as basic hacking principles, code, and examples of programming. The journal heightened the general knowledge of hacking techniques. For the most part, the members of LOD enjoyed the attention they received for their hacking activities, and they did not attempt to hide what they did from the public. Their hacking was not intended to cause harm.

However, two major members of LOD, Mark Abene (who went by the moniker Phiber Optik) and Chris Goggans (known as Erik Bloodaxe, who also served as editor of *Phrack* magazine), had a disagreement, and in 1989, Abene chose to leave (or was kicked out of) LOD to form a new group, Masters of Deception, or MOD. Members of MOD were known for hacking into networks so they could steal credit card numbers or access (and post) the credit card purchasing information of celebrities such as Julia Roberts. They also hacked into the computer system of AT&T.

The spat between LOD and MOD members continued for about two years. In the hacker circles, the argument was sometimes referred to as the "Great Hacker War." The members of each group attacked each other through the internet. They jammed each other's phone lines and even monitored the other's computer activity. Members of both groups would, on occasion, switch their allegiance to the other group or even cooperate with each other in hacking endeavors. This made it difficult to ascertain what group (or person) was responsible for hacking events.

One day, a meeting was taking place of LOD members via a hacked phone company line when a MOD member, John Lee, who went by the name Corrupt, entered the conversation. Members of LOD were upset and made some comments offensive to MOD. Lee and other members of MOD joined together to harass members of LOD, focusing their efforts on Goggans. They hacked into his phone line so they could listen to his calls, they switched his service, and called him at all hours of the day. Goggans responded by posting negative comments about MOD but ultimately called the FBI for assistance.

The FBI had already been investigating MOD alongside the Secret Service in an operation they called Operation Sun Devil. The trigger event occurred on Martin Luther King Jr. Day in 1990, people with AT&T service heard the message, "All circuits are busy now, please try later." This lasted for nine hours. About a week later, the FBI and Secret Service arrested multiple members of MOD and charged them with trespassing and computer tampering. The agents seized 42 computers and over 20,000 computer disks, along with other items that served as evidence against the hackers. The hackers stole login credentials, passwords, and other information, forcing the company to spend $3 million on increasing their network security. In the days after, LOD fell apart.

Another person associated with LOD who was investigated as part of Operation Sun Devil was Leonard Rose Jr., from Maryland, who also went by the name "Terminus." Agents searched his home and removed hundreds of items, including computers and computer disks. He was indicted on five counts of computer fraud, including the electronic transfer of a computer program that was owned by AT&T. He was sentenced to serve one year in prison.

Eventually, Abene was charged with, and pleaded guilty to, federal charges of conspiracy and unauthorized access to federal-interest computers. He later went into the computer security business with former members of LOD, after being adversaries for so long. He was later named one of New York City's 100 smartest people. The Secret Service investigated Goggans, but he never faced criminal charges. He and LOD created an Internet Security consultancy group called Crossbar Security to help any company that had been hacked by MOD. The company did not survive the dot-com bust, and Abene became an expert in computer security and often provides assessment for national companies. He also serves as a consultant to national news and media outlets, and has become an author of multiple books on network security. Lee spent time in prison and currently directs documentaries and music videos.

See also: Abene, Mark; Anonymous; Black-Hat Hackers; Chaos Computer Club; Hacker and Hacking

Further Reading

Middleton, Bruce. 2017. *A history of cyber security attacks: 1980 to present*. Boca Raton, FL: CRC Press.

Pots, Mark. 1991. "Hacker pleads guilty in AT&T case; Sentence urged for Maryland man among stiffest yet for computer crime." *The Washington Post*, March 23, 1991.

Schatz, Willie. 1990. "The terminal men: Crackdown on the 'Legion of Doom' ends an era for computer hackers." *The Washington Post*, June 24, 1990.

Slatalla, Michelle, and Joshua Quittner. 1995. *Masters of deception: The gang that ruled cyberspace*. New York: Harper Collins.

Steinberg, Steve G. 1996. "The scare stories about security miss real issue." *Los Angeles Times*, June 17, 1996.

LEGISLATION

Cybercrime legislation began in the United States in the late 1970s. The Florida Computer Crimes Act of 1978 appears to be the first piece of cybercrime legislation. It was designed to cover three specific areas of cybercrime: the infringement of intellectual property rights via computer, harm done to computers and its software, and harm done to computer users—such as being locked out of a computer (Florida Legislature, 1978). By 1981, 14 states followed Florida's lead and passed computer crime legislation (Harsch, 1981).

At that same time in the early 1980s, attempts were being made to pass federal computer crime legislation. This appears to have received some pushback from the computer industry (Harsch, 1981). This notwithstanding, work towards federal computer crime legislation was undertaken, at least in part in response to the movie *WarGames* (1983), wherein a teenage boy almost inadvertently starts nuclear war between the United States and U.S.S.R. via hacking (see Schulte, 2008).

The first piece of federal cybercrime-specific legislation—the Computer Fraud and Abuse Act of 1984—was passed shortly thereafter. The legislation was amended just two years later. Even as amended, the legislation had some limitations. The law required suspects to make unauthorized access onto a computer for it to be a crime, thus making any inside job by definition noncriminal. Also, the law did not criminalize the mere access of a computer and viewing of data on it without anything more (May, 2004).

Additional cybercrime legislation has followed. The Electronic Communications Privacy Act was passed in 1986, prohibiting the unauthorized interception of electronic communications (see May, 2004). The Digital Millennium Copyright Act was passed in 1998 to prohibit the use of certain digital tools to circumvent measures implemented by companies to protect their copyrighted material. The CAN-SPAM Act of 2003 created civil penalties for companies that engaged in deceptive e-mail advertisement practices.

The more technology advances, the more need there is for cybercrime legislation to address the new and innovative ways in which cybercriminals commit cybercrimes. It is not always necessary for states and the federal government to pass new legislation to deal with cybercrime. There are many crimes that existed before the advent of the internet but are still applicable to online behavior. For example, the possession of child pornography was illegal before the internet existed. Proliferation of child pornography is certainly still a problem online. Similarly, financial crimes such as theft and money laundering existed before the internet. The internet has simply provided a new forum to commit these crimes. Thus, old criminal legislation in many instances is still applicable to cyber situations, thus not requiring any additional legislation.

There are several categories that cybercrime legislation can fall into. First and foremost, many laws criminalize harmful online behavior. Examples of this would be state laws criminalizing the posting of revenge porn or sexting between minors—both things that the majority of states have enacted legislation on.

Second, there are online acts that are illegal but not criminal. These acts are prohibited by civil law, and violators of those laws can be face fines, injunctions, and so forth. An example of this would be cybersquatting. This is treated as a civil cause of action in the United States (U.S. Code, Title 15 § 1125(d)) and internationally (World Intellectual Property Organization, 2018). Violators may be forced to forfeit the domain name in question. A violator would not be exposed to standard criminal penalties, however, such as incarceration.

Third, there is legislation that has both criminal and civil penalties for unauthorized behavior. Copyright laws in the United States fall into this category (U.S. Code, Title 17 § 101 et seq.). Someone who intentionally infringes on another's copyright could face both criminal sanctions, as well as injunctions and the payment of damages on the civil end. The CAN-SPAM Act of 2003 in the United States also falls into this category. The act regulates the sending of commercial e-mail. Violation of some provision of the act can result in fines, while violation of other provisions can result in criminal penalties such as incarceration.

Lastly, there is another body of cybercrime-related legislation. It provides regulations for government agencies to abide by in order to protect against cybercrime. An example of this is the Cybersecurity Workforce Assessment Act. It directs the Department of Homeland Security to assess how well it is meeting its cybersecurity obligations. Legislation such as this does not necessarily provide for punishments if the tenets of the law are not fulfilled. Rather, it provides a framework an agency is supposed to operate within.

See also: CAN-SPAM Act of 2003; Computer Fraud and Abuse Act of 1986; Cybersecurity Act of 2012; Cybersecurity Enhancement Act of 2014; Cybersecurity Workforce Assessment Act of 2015; Cybersquatting; Digital Millennium Copyright Act; Financial Crimes; Florida Computer Crime Act of 1978; Fraud; Personal Data Notification and Protection Act of 2017; Punishment; Revenge Porn; Sexting

Further Reading

Florida Legislature. 1978. "Summary of general legislation 1978." Florida Legislature. https://fall.law.fsu.edu/collection/FlSumGenLeg/FlSumGenLeg1978.pdf

Harsch, Jonathan. 1981. "Computer crime: Grappling with a 'high tech' problem." *The Christian Science Monitor*, November 4, 1981. https://www.csmonitor.com/1981/1104/110433.html

May, Maxim. 2004. "Federal computer crime laws." SANS Institute Information Security Reading Room, June 1, 2004. https://www.sans.org/reading-room/whitepapers/legal/federal-computer-crime-laws-1446

Schulte, Stephanie Ricker. 2008. "'The *WarGames* scenario': Regulating teenagers and teenaged technology (1980–1984)." *Television & New Media* 9, 6: 487–513.

World Intellectual Property Organization. 2018. "WIPO cybersquatting cases reach new record in 2017." World Intellectual Property Organization, March 14, 2018. http://www.wipo.int/pressroom/en/articles/2018/article_0001.html

LEVIN, VLADIMIR (1967–)

Vladimir Levin is a Russian hacker and cybercriminal who is known for committing the first banking crimes on the internet. Levin was a math major from

St. Petersburg University who was able to use a list of stolen customer passwords to log into bank accounts belonging to patrons at Citibank 18 times over the span of a few months. He made 40 transfers, totaling over $10 million, from customer bank accounts into accounts that were set up by other cybercriminals located in Finland, the Netherlands, Israel, Germany, and the United States. Three of the conspirators were arrested as they attempted to withdraw the funds from the accounts. Each of the offenders named Levin as the architect of the scheme. Levin was employed at the time at a computer company in St. Petersburg in Russia.

In August 1994, officials working in Citibank's security system noted two transfers that seemed to be abnormal. One of the transfers was for $26,800 and the other for $304,000. Executives at the bank contacted the FBI. Agents were able to track the transfers to a Russian hacker named Vladimir Levin. Officials arrested Levin in Heathrow airport in London. He fought extradition to the United States for two and a half years (because Russia had no extradition treaty with the United States) before being transferred to the United States to face charges. In 1988 he agreed to a plea bargain in which he pleaded guilty in the U.S. District Court for the Southern District of New York to one count of conspiracy to defraud and to the theft of $3.7 million. He was sentenced to three years in prison and ordered to pay restitution of $240,015. Four of the other offenders pleaded guilty for criminal charges of conspiracy to commit bank fraud, each serving a sentence in prison.

In the end, Citibank retrieved all but $400,000 of the stolen funds. Levin's crimes were indicative of the harm that can occur if financial data is not well protected, and they showed that banks and other institutions can be vulnerable to cybercriminals. It also pointed to the need for increased computer security to protect against these or similar crimes. The case was also responsible for the loss of the public's confidence in the online banking system. Many banking institutions worked quickly to improve their online security systems.

See also: Banking Attacks; Black-Hat Hackers; Economy, Effects on; Hacker and Hacking

Further Reading

Dow Jones Newswires. 1998. "Russian hacker is sentenced to 3 years in Citibank heist." *Wall Street Journal*, February 24, 1998. https://www.wsj.com/articles/SB888360434859498000

Hansell, Saul. 1995. "Citibank fraud case raises computer security questions." *New York Times*, August 19, 1995. https://www.nytimes.com/1995/08/19/business/citibank-fraud-case-raises-computer-security-questions.html

Harmon, Amy. 1995. "Hacking theft of $10 million from Citibank revealed." *Los Angeles Times*, August 19, 1995. http://articles.latimes.com/1996-08-19/business/fi-36656_1_citibank-system

Johnston, David Cay. 1995. "Russian accused of Citibank computer fraud." *New York Times*, August 18, 1995. https://www.nytimes.com/1995/08/18/business/russian-accused-of-citibank-computer-fraud.html.

LIZARD SQUAD

The Lizard Squad is a black hat hacking group led by Vinnie Omari, whose members have participated in a variety of hacking events since being formed. They may be most widely known for a hack on Sony PlayStation Network and Microsoft Xbox Live on Christmas Day, 2014, that brought down the systems and prevented many players from logging on to enjoy their new video games.

This is not the only attack the group's membership carried out in 2014. That year, about 60 customers of ISP Cox Communications were informed that an employee at the company had been fooled by a phishing attack and gave out personal information pertaining to the patrons. Cox was fined $595,000 for not keeping the information secure. The person behind the attack, Evil Jordie, was a member of the Lizard Squad. He called the Cox employee and acted as if he was in the company's IT department. The employee provided Evil Jordie with account IDs, passwords, addresses, and driver's license numbers, among other items. Evil Jordie then posted the information online for all to see.

In August of that year, members posted on their Twitter account that there was a bomb on an American Airlines flight, forcing pilots to make an emergency landing despite the lack of an actual explosive. This event raised the interest of the Federal Bureau of Investigation (FBI). The group continued its hacking activities in 2015. That year, members of the group carried out an attack on the website for Malaysia Airlines so that anyone entering the site received a message that said "404—plane not found." Other potential customers saw the message "ISIS WILL PREVAIL." They also decided to hack into the social media accounts owned by pop singer Taylor Swift. They threated to post photos of Swift unless she paid them a ransom of Bitcoins. However, the group did not actually possess compromising photos of Swift.

After these hacking actions, the FBI and other law enforcement agents investigated the hacking of Lizard Squad members. They arrested one of the founding members of the group, Zachary Buchta from Maryland. He pleaded guilty to one count of conspiracy to commit damage to protected computers and was later sentenced in federal court to three months in prison. He was also ordered to pay $350,000 in restitution to two online gambling companies. He harassed any person online, a service he provided in exchange for a $20 fee. Victims would receive harassing phone calls filled with swearing. One victim received a call every hour for 30 days in a row.

Other members of Lizard Squad were also arrested. One of those, Julius Kivimki, from Finland, (who went by the name zeekill), was charged with over 50,000 computer crimes and convicted of those in July of 2015. Another member who was charged with crimes was Bradley Jan Willem van Rooy, a 19-year-old from the Netherlands, who was known as "UchihaLS." He was charged with computer crimes after carrying out distributed denial-of-service (DDoS) attacks and stealing credit card information.

See also: Black-Hat Hackers; Denial-of-Service Attack (DoS); Federal Bureau of Investigation; Hacker and Hacking

Further Reading

Fung, Brian, and Andrea Peterson. 2014. "Meet the Grinch who stole Christmas for gamers: The Lizard Squad." *The Washington Post*, December 26, 2014. https://www.washingtonpost.com/news/the-switch/wp/2014/12/26/meet-lizard-squad-the-group-claiming-responsibility-for-ruining-christmas-for-gamers/?utm_term=.803fa34a91c3

Meisner, Jason. 2018. "'Lizard Squad' hacker-for-hire cries in court as he's sentenced to three months in prison." *Chicago Tribune*, March 28, 2018. www.chicagotribune.com/news/local/breaking/ct-met-hacker-zachary-buchta-sentenced-20180327-story.html

Raghuvanshi, Gaurav, Newley Purnell, and Jason Ng. 2015. "Malaysia Airlines website hacked by group calling itself 'Cyber Caliphate.'" *The Wall Street Journal*, January 26, 2015. https://www.wsj.com/articles/malaysia-airlines-website-hacked-by-group-calling-itself-cyber-caliphate-1422238358

Turton, William. 2014. "An interview with Lizard Squad, the hackers who took down Xbox Live." *The Daily Dot*, December 26, 2014. https://www.dailydot.com/debug/lizard-squad-hackers/

LLOYD, TIMOTHY (1967–)

Timothy Lloyd is a former employee of Omega Engineering Corporation—a company that manufactured control equipment and industrial process measurement devices. Its customers included the National Aeronautics and Space Administration (NASA) and the United States Navy (PBS, 2019; Gaudin, 2000). Lloyd worked for Omega for 11 years and ultimately became a network administrator for the company. He was fired on July 10, 1996, for behavioral and performance issues (Department of Justice, 2002; Gaudin, 2000). Lloyd installed a logic bomb in the computer network that was set to detonate on July 31, 1996. The logic bomb did activate at that time, deleting all the software programs the company used. This cyberattack resulted in a loss of $10 million to Omega (Department of Justice, 2002). According to the Secret Service—the agency that investigated the attack—this was the largest incident of computer sabotage initiated by an employee at the time (Department of Justice, 2002; PBS, 2019).

The attack by Lloyd was set up via a logic bomb with a time-based trigger to activate on July 31, 1996. This was installed on Omega's computer network before Lloyd's last day. Before his last day, Lloyd took other steps to ensure the success of his cyberattack. He deleted the software from the individual workstation computers and left sole copies of the software on one server—the server that was attacked on July 31, deleting all the software. Lloyd also stole the backup tapes that could have been used to reinstall the software before his last day. Those tapes were ultimately found in Lloyd's home when the Secret Service executed a search warrant there less than a month later. The data from the tapes had been erased (Gaudin, 2000). Investigators were ultimately able to trace the attack back to six lines of code—the logic bomb—that was designed to delete all the software (Gaudin, 2000; PBS, 2019).

Lloyd was charged with computer sabotage and transporting stolen equipment from Omega to his residence (Department of Justice, 2002). Lloyd contested the charges, and his case went to trial. His defense was that Omega—who had not yet hired a network administrator in the wake of Lloyd's firing—was using him as a scapegoat for their own negligence. The State provided evidence of the tapes found in Lloyd's house, evidence that Lloyd was the employee that was in charge of the computer network prior to his termination, and evidence of Lloyd's motive. Prior to his firing, Lloyd's role with Omega shrank, and Lloyd acted out by physically intimidating coworkers. This ultimately led to his firing (Gaudin, 2000; *United States v. Lloyd*, 2001). The state argued the cyberattack was Lloyd's retaliation for the firing. The jury appears to have believed the State, and convicted Lloyd of computer sabotage on May 9, 2000 (PBS, 2019). However, it did acquit him of the charge of transporting stolen equipment (Department of Justice, 2002). Lloyd's conviction was momentarily set aside by the trial judge. This was due to a juror expressing concern that her vote in jury deliberations may have been influenced by a television program she had viewed about a computer virus. The appellate court ultimately reinstated the conviction (*United States v. Lloyd*, 2001). Lloyd was sentenced to 41 months in prison on February 26, 2002 (Department of Justice, 2002).

See also: Logic Bomb; Secret Service; Virus

Further Reading

Department of Justice. 2002. "Former computer network administrator at New Jersey high-tech firm sentenced to 41 months for unleashing $10 million computer 'Time Bomb.'" February 26, 2002. https://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/lloydSent.htm

Gaudin, Sharon. 2000. "The Omega files: A true story." CNN, June 27, 2000. http://www.cnn.com/2000/TECH/computing/06/27/omega.files.idg/

PBS. 2019. "Notable hacks." PBS. https://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/notable.html

LOGIC BOMB

A logic bomb is malware that is activated upon the occurrence of some event. Some logic bombs are designed to activate at a specific date and time. Accordingly, these types of logic bombs are sometimes referred to as time bombs. Other activating events include logging onto the internet, logging onto specific websites, and removal of information from a computer or computer network. A logic bomb can carry out various functions. Working by itself, a logic bomb may be designed to delete information from the infected computer. This may happen with employees who place a logic bomb in their employer's computer network. The logic bomb can be programmed to delete information from the network in the event that employee is fired—the triggering event being the removal of the employee from the company's payroll database (Armendariz, 2019). Logic bombs can also work in conjunction with other malware. One possible pairing is a logic bomb with a keystroke monitor. A keystroke monitor keeps a record of every key pressed on a keyboard of an infected computer. These are used to detect the usernames and passwords of victims to gain unauthorized access to the victim's online accounts. To more easily detect a username and password, a keystroke monitor may be set to operate through a logic bomb, only tracking the keystrokes of a victim after they have visited a specified website, such as an e-mail or bank website (Armendariz, 2019). This limits the amount of text from a keystroke monitor a cybercriminal will have to sift through to find a victim's username and password.

One possible advantage to cybercriminals of using a logic bomb is the ability to carry out coordinated attacks on several targets simultaneously. If a cybercriminal were to attack several targets using the same malware in an asynchronous manner, there is a risk that following the attack on the first target, a safeguard against that malware will be discovered and implemented by potential future targets before the cybercriminal can attack them. However, if the target computers are all infected with a logic bomb, and the computers are all attacked at the same time, there will be no time for such a response. A widespread coordinated attack using a logic bomb occurred in South Korea in 2013. The logic bomb in that instance was used to attack banks and media companies in South Korea. The logic bomb was activated at 2:00 p.m. (local time) on March 20 of that year, hitting at least five companies simultaneously. Once activated, the logic bomb began erasing data from those companies' computers (Zetter, 2013).

Another possible advantage to cybercriminals of using a logic bomb is the ability to have the malware take affect only after the cybercriminal has left the scene. This would apply to instances where the cybercriminal would have physical access to the computers being attacked and would need to leave the scene. This can be seen, as mentioned above, in instances where a soon-to-be-former employee installs a logic bomb on the computers of their soon-to-be-former employer. In 2008, Rajendrasinh Babubhai Makwana—an employee of Fannie Mae—installed a logic bomb on Fannie Mae's computers the day he was fired as a contractor for the company in 2008. The logic bomb was designed to activate three months after his firing, and to delete all data on the system. The logic bomb was discovered before it activated. In 2010, Makwana was sentenced to 41 months in prison (United States Attorney's Office, 2010). In a similar incident in 2014, Mittesh Das—a contractor with the U.S. Army—installed a logic bomb on the army's computers. Das did this after being outbid by another contractor and losing his contract with the army. Days before the changeover, Das uploaded the logic bomb. The day after the changeover was complete, the logic bomb activated. Das was sentenced to two years in prison in 2018 (United States Attorney's Office, 2018).

See also: Keystroke Monitoring; Malware; Spyware; Virus; Worm

Further Reading

Armendariz, Tommy. 2019. "What is a logic bomb?" *Lifewire*, March 4, 2019. https://www.lifewire.com/what-is-a-logic-bomb-153072

United States Attorney's Office. 2010. "Fannie Mae corporate intruder sentenced to over three years in prison for attempting to wipe out Fannie Mae financial data." Federal Bureau of Investigation, December 17, 2010. https://archives.fbi.gov/archives/baltimore/press-releases/2010/ba121710.htm

United States Attorney's Office. 2018. "Georgia man sentenced for compromising U.S. Army computer program." Department of Justice, September 11, 2018. https://www.justice.gov/usao-ednc/pr/georgia-man-sentenced-compromising-us-army-computer-program

Zetter, Kim. 2013. "Logic bomb set off South Korea cyberattack." *Forbes*, March 21, 2013. https://www.wired.com/2013/03/logic-bomb-south-korea-attack/

LULZSEC

LulzSec, or Lulz Security, was a hacking group comprising former members of the group Anonymous who split from that group in 2011. The group was formed on May 15, 2011 with the goal of having fun by causing mayhem. LulzSec was allegedly created in a private online chat room of Anonymous. There were seven primary members of the group. One of the founders, Hector Monsegur, also known online as Sabu, was the group's leader and an experienced hacker.

The LulzSec motto was "Laughing at your security since 2011." The name is a combination of "lulz," which comes from "laugh out loud," and "Sec," or security. Their logo was a stick man with a mustache and a monocle, top hat, and three-piece suit; usually, he was sipping a glass of wine. The logo eventually became known as "the Sir." The group existed for only two months, falling apart after the Federal Bureau of Investigation arrested Monsegur in 2011. Following his arrest, Monsegur became an informant for the agency while continuing to maintain his persona as Sabu with other members of LulzSec. He reported back to the FBI concerning any conversations he had with other members or activities they were pursuing.

The group claimed that they only hacked sites to get attention and to make people aware of lax security systems. In doing so, they launched DoS attacks on companies that diverted so much internet traffic to a website that it became inoperable. They sometimes stole personal information from networks that had weak security systems and published that personal information, unencrypted and readily available, on the internet. It is alleged that the group is responsible for causing billions of dollars in damages to the companies they attacked.

The group was more secretive than Anonymous. The members did not give any information to journalists and in general gave no interviews. They did not discuss their hacking activities. The members of LulzSec carried out some high profile attacks. For example, in 2011 they targeted Sony Music Entertainment Japan, Sony Pictures Entertainment, and the Sony PlayStation network, which took the site offline for many days. The group also stole $24.6 million items of personal data from customers. In the end, it is estimated that the attack cost the company $20 million.

Other attacks that were carried out by LulzSec in 2011 included those directed toward the Arizona Department of Public Safety, the U.S. Senate, the UK Serious Organised Crime Agency Bethesda Softworks, AOL, and AT&T. That same year, when *PBS Frontline* aired a segment on WikiLeaks and Chelsea Manning called "WikiSecrets," members of LulzSec hacked into the site and defaced it, leaving behind a fake article claiming that Tupac Shakur and Biggie Smalls were alive and living in New Zealand. An attack on the website of Fox Broadcasting System ended with altering the LinkedIn profiles of many employees and publication of passwords and contact information of 73,000 contestants of the television talent show *X Factor*. LulzSec also claimed to have taken the Central Intelligence Agency (CIA) website offline for a short period.

On June 26, 2011, members of LulzSec published a statement in which they admitted that the organization consisted of six members. The group then unexpectedly broke up. But on July 28, the group hacked into the online site for the UK newspaper *The Sun* and altered the page so that visitors were re-directed to a fake news story that the owner of the paper, Rupert Murdoch, had died in his home of a drug overdose. The story, with the headline "Media Mogul's Body Discovered," falsely informed readers that Murdoch had ingested a large amount of palladium in his topiary garden.

The group formally fell apart in 2011 when Monsegur (Sabu) was arrested and subsequently turned in other members of the group to law enforcement. He pleaded guilty to several charges, including hacking, bank fraud, and identity theft. He agreed to cooperate with the FBI in exchange for a reduced sentence. He helped the FBI identify the other members of the group, but he also helped the FBI identify members of Anonymous and another group named the Internet Feds. He also helped to prevent other hacking events that were in the planning stages.

Other members of LulzSec included Jake Davis, who was also known as Topiary. Davis was a former member of Anonymous. He operated the Twitter account for LulzSec and also wrote the group's press releases or appeared for interviews with the media. Davis was arrested in 2011 and charged with five counts of unauthorized access of a computer and conspiracy. He pled guilty to two counts of conspiracy to do an unauthorized act with the intent to impair the operation of a computer. He was sentenced to 24 months in a young offender's facility.

Another member was Ryan Ackroyd, also known as Kayla/KMS. Ackroyd was a former member of the British army and a skilled hacker. He was responsible for researching the attacks that LulzSec carried out. He was arrested in 2012 on conspiracy and was sentenced to 30 months in prison.

Tflow, or Mustafa Al-Bassam, acted as the web developer for LulzSec. He was in charge of security and maintenance and was able to identify websites with vulnerabilities that could be exploited. He was arrested in July 2011, but because he was underage when he committed his offenses, he was sentenced to only 20 months in a facility, which was suspended for two years, and 300 hours of community service.

Other members included Darren Martyn, referred to as Pwnsauce. A native of Ireland, Martyn was indicted in 2012 on charges of conspiracy. Another Irish offender was Palladium, whose real name was Donncha O'Cearbhaill, and he was indicted in 2011 of conspiracy charges. Anarchaos, whose real name was Jeremy Hammond, was from Chicago. He was arrested on hacking charges.

ViraL, a nickname for Ryan Cleary, was originally from Essex, England. He had control of a botnet through which he could control 100,000 computers. He sometimes rented out the botnet to others, who then launched DoS attacks. He was sent to jail for two years and 8 months in 2013 for hacking into the CIA, the Pentagon, SONY, Nintendo, the Arizona State Police, 20th Century Fox, PBS, and other groups. In 2013, Cleary was accused of having over 170 lewd images of children on his computer.

The activities of LulzSec have made many people and organizations more aware of the need for more secure computer systems. They often chose to attack websites that had little security. They would steal information and then post it online.

See also: Anonymous; Cleary, Ryan; Hacker and Hacking; Legion of Doom; Lizard Squad; Sony Pictures Entertainment Hack

Further Reading

Arthur, Charles. 2013. "LulzSec: What they did, who they were and how they were caught." *The Guardian*, May 16, 2013 https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail

Cluley, Graham. 2013. "The LulzSec hackers who boasted they were 'Gods' await their sentence." Naked Security, May 16, 2013. https://nakedsecurity.sophos.com/2013/05/16/lulzsec-hackers-wait-sentence/

Coleman, Gabriella. 2014. *Hacker, hoaxer, whistleblower, spy: The many faces of anonymous*. London: Verso.

Essany, Michael. 2012. *LulzSec: How a handful of hackers brought the US government to its knees: 50 days of Lulz*. New York: Hyperlink.

Leyden, John. 2013. "Who is the mystery sixth member of LulzSec?" *The Register*, May 17, 2013. https://www.theregister.co.uk/2013/05/17/lulzsec_analysis/

"LulzSec's Ryan Cleary admits hacking into CIA and the Pentagon." 2012. *The Telegraph*, June 25, 2012. http://www.telegraph.co.uk/technology/news/9354188/LulzSecs-Ryan-Cleary-admits-hacking-into-CIA-and-the-Pentagon.html

Rawlinson, Kevin. 2013. "LulzSec hacker Ryan Cleary will be freed 'imminently' despite 170 child sex abuse images." *The Independent Online*, June 12, 2013. http://www.independent.co.uk/news/uk/crime/lulzsec-hacker-ryan-cleary-will-be-freed-imminently-despite-170-child-porn-images-8655209.html

Sweatman, Will. 2016. "The dark arts: Meet the Lulzsec hackers." *Hackaday*, January 26, 2016. https://hackaday.com/2016/01/26/the-dark-arts-meet-the-lulzsec-hackers/

M

MALWARE

The term "malware" refers to any type of malicious software program or code that is used to infiltrate networks and computers in order to cause damage or to gain access to, or steal, private information or data. Most malware relies on unknown vulnerabilities, or a flaw in the program, that leaves an opening that criminals use as an entry to the networks. Once a criminal finds their way into a system, they can upload the malware.

Malware is often attached to online advertisements. When the victim clicks on an ad, malware is loaded onto the computer. The victim will be unaware that the malware has been uploaded so they continue to use it as normal. While they do that, the offender is collecting passwords, personal information, credit cards, and other types of data that can be used by the criminal.

Malware is more readily available today than ever before, posing serious implications for governments, businesses, and individuals. Many kinds of malware are available to rent or to purchase online, particularly on the dark web. It is easy to purchase exploit kits and botnets that can be used to carry out an attack. It is not necessary that an offender has the technical skills to write code to implement malware. This means that cybercriminals only need to have enough Bitcoins or some other cryptocurrency to carry out an attack. In addition, those interested in using the malware is growing, along with members of the hacking community who are able to create different forms of malware. Malware for mobile devices is becoming more popular since just about everyone has a mobile phone.

Types of Malware

Ransomware

Ransomware is a form of blackmail whereby an offender threatens to lock a computer system unless a ransom is paid. This is usually a financial ransom, often paid for in Bitcoins or other online currency. Many hospitals and police departments, or other agencies that need immediate use of their files, end up paying the ransom. Individuals who face a loss of digital personal property, personal banking, or medical information will also pay the ransom.

Worms

Worms are malware that infect a computer and cause the computer or network to slow down. In some cases, the worm causes a network to shut down. An example of this malware is the Morris Worm, which was a self-replicating virus that was loaded into the operating system of a network. It made infected computers slow down because it used the computer's resources to replicate itself. The worm was installed when a user opened an e-mail or an attachment. The worm looked for a vulnerability to get inside the computer and, once inside, sent infected e-mails to the contacts in the address book.

It can be difficult to remove a worm from a computer. Worms generally do not need to attach themselves to a particular file and do not have the goal of modifying any code. Instead, it copies itself into the computer's memory and then uses the e-mail address book to send e-mails to other systems.

The first computer worm was the Creeper virus that spread through ARPANET, the precursor of the internet. The virus was the first malware of its kind to exist. Bob Thomas originally created the virus in 1971 and named it after a character on the cartoon *Scooby-Doo, Where Are You!* A computer infected with the virus displayed the message, "I'm the creeper: catch me if you can." Thomas created the self-duplicating program as an experimental program and had no intention of causing damage to other computers. Luckily, the virus did not cause significant damage, but some claimed that it replicated itself so often that other programs could not run. Most people at the time considered it to be more of a nuisance. Another virus, called the Reaper, was created as a way to delete the Creeper on infected computers.

Koobface

Koobface is the name of a computer worm that attacked Microsoft Windows, Mac OS X, and Linux platforms. It has also been used to launch attacks on the computers of users of social network sites such as Facebook, Twitter, Skype, or other sites including MSN, AOL Mail, Yahoo Mail, and Gmail. It was first detected in August 2008 and then again in March 2009. Koobface is an anagram of Facebook.

When cybercriminals are able to upload the worm onto a computer, the machine turns into a zombie computer, so the offender has control over it and is able to access files. This then allows the offender to steal personal data, such as login information or financial information. Koobface will also display ads, links, and fake messages on the infected computer, all of which help to spread the virus to others. If an unsuspecting user clicks on a link that takes them to a fake YouTube or Facebook video, the user will then get the virus. Koobface will also contact other compromised computers and create a botnet so the offender will have an army of computers under his or her control.

The people who were responsible for the worm were located in St. Petersburg, Russia, and they went by the moniker "Ali Baba $ 4." Their names were Stanislav Avdeyko (leDed), Alexander Koltyshev (Floppy), Anton Korotchenko (KrotReal), Roman P. Koturbach (PoMuc), and Svyatoslav E. Polichuck (PsViat and PsychMan).

To prevent the spread of Koobface or other worms, it is essential that a user install any patches that are available and keep an antivirus software updated. Users must also be cautious about the sites they visit and refrain from downloading software unless it is from a known source. If any malware is discovered on a computer, it should be removed immediately.

Viruses

Viruses are an older form of malware, but are still used today. A user must open a file or an attachment that contains the virus in order for their computer to be infected. When that file is opened, the virus is quickly installed on the computer. The end result of a virus depends on how that virus was written. Some have allowed the offender controlling the malware to access data, steal data, or corrupt files (and make them unusable).

Many viruses have appeared on computers worldwide. One of the earliest was the Wabbit virus, which was first detected in 1974. It was also a self-replicating virus that made copies of itself and did not stop until it bogged down a computer, resulting in the computer crashing. The virus was named the Wabbit (rabbit) because of how quickly it could replicate itself. In 1981, the Elk Cloner, written by 15-year-old Rich Skrenta, infected the memory on Apple II computers. On every 50th boot, a poem would be displayed. In 1986, the Brain Boot Sector virus, written for the MS-DOS and the IBM PC compatible virus, was discovered. Users whose machines were infected received the message: "Welcome to the Dungeon. . . . Beware of this VIRUS. . . . Contact us for vaccination."

Exploits

Exploits use a weakness in the security system to install malware. Once the exploit finds a vulnerability, the malware allows an offender to take control of a computer so that files can be stolen or the computer used for a DoS attack.

Bots

A bot is a type of malware that allows an offender to control the computer from afar. Botnets are a collection of infected machines that can be controlled by a cybercriminal who is known as the botmaster. The botmaster controls the actions of the infected computer, called a zombie computer. The botmaster will often make the computer perform illegal actions, such as sending private information to the botmaster. It can also be used to download other malware on the already infected computers.

The malware known as a botnet is available for a person to purchase or rent. This means that people with little technological background could easily use them to commit cybercrimes. They can steal information and sell it quickly on the dark web. Today's bots are larger and more complicated now than they used to be. They can infect millions of machines quickly, giving the botmaster a lot of control over many computers. This can cause a great amount of harm around the world in a very short time.

Trojan Horses

A Trojan horse installs applications on a computer so that hackers are able to control it from afar. Trojan horses allow an offender to steal files or cause damage to a computer. Most Trojan horses are embedded in a software program or attachment that appears to be a safe, downloadable file. It may be photos or e-mails from friends. When the user uploads the software, the malware will also install itself.

Once on the computer, it will run automatically to delete files, log the keystrokes a victim uses, and keep track of usernames and passwords.

Phishing

Phishing is a way for hackers to steal information. This is often carried out via a false website that appears to be legitimate. It can also be a false e-mail or attachment. The false website or e-mail asks the use to give their data, maybe because some records were lost, or the system is being updated, or some other falsehood. Victims may give their personal information, allowing the offender to use the information to log onto a system or network. In the past, phishing attacks have allowed cybercriminals to steal funds from bank accounts.

E-mail Scams

E-mail scams trick the victim with a fake promotion of some kind, via e-mail, asking the victim to pay money in order to obtain a prize or some other award. Some e-mail scams, referred to as Nigerian scams because they often originate in that country, revolve around a wealthy individual who needs money to escape the country. If the victim sends money, they are promised to receive part of the individual's inheritance or wealth. Of course, this money is never received by the victim. Romance scams are similar. A victim may find a romantic partner on a dating site who claims to need money to pay for travel expenses to see the victim. The victim sends the money, but the romantic partner never appears.

Keylogger and Spyware

A keylogger is a type of malware that collects all keystrokes and computer activities that are made by a user. When a user logs on to a banking site to access their financial records, or purchases items online, the cybercriminal collects all of that information and uses it to steal from the victim or sells the information to other criminals. Some malware take screenshots of a computer at regular intervals and transmit them to the offender.

Similar to keyloggers, spyware gathers names, passwords, and other confidential information from a user. Some spyware, called password stealers, focuses on gathering a person's login credentials, whereas other spyware gathers banking or financial information.

Advanced Persistent Threat (APT)

Advanced persistent threat is malware that monitors a company's security and works to continually steal information from a computer or network over a longer period of time. It is essential that the malware remain undetected for the attack to be considered successful.

Easter Egg

The term "Easter egg" refers to an unexpected, harmless surprise that has been hidden in computer software that has been placed there by a programmer. Some Easter eggs give credit to the software developer, whereas others can be jokes, sound effects, or animation. They are usually hidden and largely unknown to most users. An example of an Easter Egg is found in the 1988 movie *The Wizard of Speed and Time*. After one of the animators working on the film was notified and told that he would not receive credit for his work on the film, other animators and filmmaker Mike Jittlov chose to spell the animator's name out using marching toys in one of the movie's scenes (Kay, 2000). Most viewers of the film do not recognize the word spelled out by the toys.

Critics of Easter eggs claim that programmers who are creating the surprises will delay the release of the movie and other products because they are spending time creating the hidden surprises. Some critics argue that the surprise Easter eggs take up extra, unneeded disk space, meaning that the program will take longer to install. In 2002, Microsoft banned the practice of adding hidden code to programs through something called the Trusted Computing Initiative. In making the new rules, Microsoft explained that Easter eggs and hidden codes can lead to security issues. Some hidden code can contain malware, spyware, or otherwise be intended to cause harm. For example, a TSA agent place hidden code into the TSA computer system as a way to sabotage the terrorist screening database used by the TSA. Hidden code placed by an IT contractor for the mortgage bank Fannie Mae was intended to delete customer's data (Bar-Yosef, 2012).

Law Enforcement Responses

Many malware threats are now blended threats that combine different aspects of these malware forms into one attack. So, for example, a botnet will use both a Trojan horse and spyware on a victim. Once the bot infects the computer, the Trojan horse and spyware will allow the offender to gather a great deal of information from the victim.

It is difficult for law enforcement to eradicate malware available to carry out an attack. While law enforcement has intensified their online activities to collect evidence against offenders, it is a difficult task to go after cybercriminals. If an offender is arrested, there are others who step up to replace them. As the internet continues to grow, the number of offenders is denial-of-service attacks, and spyware. Moreover, stolen data is also readily available.

It is essential that users know how to prevent malware from being placed in their computers or system so that their data and files can remain confidential. To do this, antivirus software should be placed on the computer that will detect and, if needed, remedy any malware that may be on the computers. A firewall can also be part of a computer's security system. This is a software program that screens out hackers, viruses, worms, and other forms of harmful malware. It is essential that users know how to recognize e-mails that may include malware. Company employees and personal users should know not to open e-mails or attachments from unknown senders, or to refrain from going to websites that are not secure. It is also a good idea to refrain from using unsecured Wi-Fi that is available in restaurants, hotels or airports. This is a great place for cybercriminals to access unprotected computers.

See also: Advanced Research Projects Agency Network; Bitcoin; Bots and Botnets; Dark Web; Denial-of-Service Attack (DoS); E-mail-related Crimes; Exploit Kit; Morris, Robert Tappan

Further Reading

Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay. 2014. *Markets for cybercrime tools and stolen data*. Washington, D.C.: Rand Corporation.

Bar-Yosef, Noa. 2012. "Examining the threat of Easter eggs." *Security Week*, April 11, 2012. http:/www.securityweek.com/examining-threat-easter-eggs.

Elisan, Christopher C. 2015. *Advanced malware analysis*. New York: McGraw-Hill.

Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. 2018. *Cybercrime and digital forensics*. New York: Routledge.

Kay, Russell. 2000. "How to: Easter eggs." *Computerworld*, September 18, 2000. https://www.computerworld.com/article/2597221/app-development/easter-eggs.html

Musgrove, Mike. 2008. "That 'friend' may be a worm; Facebook, MySpace users hit by software carrying spam." *The Washington Post*, August 26, 2008.

Q&A about the Koobface virus. "NakedSecurity." https://nakedsecurity.sophos.com/questions-and-answers-about-koobface/

Richmond, Riva. 2010. "Attacker that sharpened Facebook's defenses." *New York Times*, November 14, 2010. https://www.nytimes.com/2010/11/15/technology/15worm.html

Sidel, Robin. 2016. "Mobile bank heist: Hackers target your phone: Malicious programs with names like Acecard and GM Bot gain popularity with thieves." *Wall Street Journal*, August 26, 2016. https://www.wsj.com/articles/mobile-bank-heist-hackers-target-your-phone-1472119200

Skoudis, Ed, and Lenny Zeltser. 2003. *Malware: Fighting malicious code*. Upper Saddle River, NJ: Prentice Hall.

Timberg, Craig, Griff Witte, and Ellen Nakashima. 2017. "Malware, described in leaked NSA documents, cripples computers worldwide." *The Washington Post*, May 12, 2017. https://www.washingtonpost.com/world/hospitals-across-england-report-it-failure-amid-suspected-major-cyber-attack/2017/05/12/84e3dc5e-3723-11e7-b373-418f6849a004_story.html?utm_term=.7f2c4305ba5f

Totty, Michael. 2011. "The first virus . . . and other not-so-great moments in the history of computer mischief." *Wall Street Journal*, September 26, 2011. https://www.wsj.com/articles/SB10001424053111904265504576568770117066288

Weaver, Nicholas. 2001. "A brief history of the worm." Symantec, November 26, 2001. https://www.symantec.com/connect/articles/brief-history-worm

MANNING, CHELSEA (1987–)

Chelsea Manning is an activist and a government whistleblower. She was born on December 17, 1987, in Crescent, Oklahoma. As a teenager, she lived for a time—from 2001 to 2005—with her mother in Wales. She returned to the United States to live with her father and stepmother for a time, and then she lived with her aunt in Maryland. While living with her aunt, Manning saw a therapist, and for the first time, she considered transitioning to presenting as female (Heller, 2017). Instead, Manning enlisted in the U.S. Army in 2007, in part as an attempt to "man up" (Shaer, 2017).

Manning attended military intelligence school at Fort Huachuca in Arizona in 2008. Manning's first duty station was in Fort Drum in New York. In 2009, she was deployed to Iraq. In her role as an intelligence analyst, Manning saw firsthand the way the United States was handling the war, and it concerned her. She considered leaking documents that showed some of the documents of concern to her. Before heading back to the United States for a two-week period of leave, Manning downloaded those documents to her laptop computer. While in the United States, she attempted to have the documents published through the *New York Times* and the *Washington Post* but was unable to make arrangements with either outlet to do so. She ultimately sent the documents to WikiLeaks on February 3, 2010 (Shaer, 2017). In a text file accompanying the leaked documents, Manning said, "This is possibly one of the more significant documents of our time removing the fog of war and revealing the true nature of twenty-first century asymmetric warfare. Have a good day" (Shaer, 2017).

Among those leaked documents was footage from U.S. military helicopters in 2010 showing U.S. military personnel killing several civilians in New Baghdad, Iraq, including journalists (WikiLeaks, 2010). The documents began being published in April, 2010. In May, 2010, Manning began communicating with a hacker named Adrian Lamo. In those communications, Manning admitted to being involved in leaking documents to WikiLeaks (Hansen, 2011). Unbeknown to Manning at the time, Lamo was working with the FBI, and ultimately turned her in (Cadwalladr, 2018).

Manning was arrested on charges related to the leaked documents on May 27, 2010. She was initially held in custody at Camp Arfijan in Kuwait and then transferred to the marine base at Quantico. She spent nine months there in a form of solitary confinement, only being allowed to leave her room one hour a day. Following criticisms of the conditions of Manning's detention, she was transferred to the Midwest Joint Regional Correctional Facility at Fort Leavenworth. There, she was allowed to be with the general inmate population (Shaer, 2017).

Manning was charged in a military court with various crimes for disclosing documents. The most serious of those charges was aiding the enemy, a charge that carries the potential of the death penalty. In addition to that, Manning was charged with multiple counts of violating the Espionage Act, five counts of theft, two counts of computer fraud, and multiple military infractions (BBC News, 2013). Manning pleaded guilty to 10 of the 22 charges against her, namely the charges alleging she leaked documents to WikiLeaks. However, Manning contested the others, including the charge of aiding the enemy (Pilkington, 2013). At trial, a military judge convicted Manning of the majority of the remaining charges—10 of the remaining 12. However, Manning was acquitted of aiding the enemy (Jones and Szoldra, 2017; Kelley, 2013). She was sentenced to 35 years in prison. The day after she was sentenced, Manning officially came out as transgender (Heller, 2017; Cadwalladr, 2018). Her sentence was later commuted on January 17, 2017, by President Barack Obama. She is now out of custody (Savage, 2017).

After being released from prison, Manning has made a living through speaking engagements. She also ran for a U.S. Senate seat in Maryland in 2018 but lost in the Democratic primaries (Cadwalladr, 2018; Fritz, 2018). In early 2019, Manning landed in custody again for refusing to testify before a federal grand jury about WikiLeaks and Julian Assange. Manning was ordered to remain in custody until she changed her mind and agreed to testify, or until the grand jury concluded its investigation (Bach, 2019). The time that grand jury was required to serve expired, and Manning was released from custody. However, a new grand jury was impaneled shortly thereafter and resumed the investigation against WikiLeaks and Assange. Manning was again summoned to testify before the new grand jury, and she again refused. In May 2019, she was again incarcerated for her failure to comply with the request of the grand jury (Ingber, 2019). She remained in custody even though an indictment against Assange was issued while she was still in custody for failing to testify to the grand jury in their investigation against him (United States Department of Justice, 2019).

The public's view of Manning is polarized. Some view Manning as a traitor. This claim was the underpinning of Manning's court martial, and some—such as President Trump—have outright called her a traitor. Others view Manning as a hero. The city of Berkeley, California was scheduled to vote on a resolution recognizing Manning as a hero back in December 2010 before the matter was ultimately tabled (Valencia, 2010). Manning herself denies she is a traitor. However, she does not refer to herself as a hero, either (Selk, 2017).

See also: Assange, Julian; Snowden, Edward; WikiLeaks

Further Reading

Bach, Natasha. 2019. "Chelsea Manning is back in jail after she refuses to testify on Wikileaks." *Fortune*, March 8, 2019. http://fortune.com/2019/03/08/chelsea-manning-jail-refuses-to-testify/

BBC News. 2013. "Wikileaks source Manning convicted on most charges." July 30, 2013. https://www.bbc.com/news/world-us-canada-23506213

Cadwalladr, Carole. 2018. "'I spent seven years fighting to survive': Chelsea Manning on whistleblowing and WikiLeaks." *The Guardian*, October 7, 2018. https://www.theguardian.com/us-news/2018/oct/07/chelsea-manning-wikileaks-whistleblowing-interview-carole-cadwalladr

Fritz, John. 2018. "8 years after leaking thousands of classified documents, Chelsea Manning is running for U.S. Senate in Maryland." *Baltimore Sun*, February 20, 2018. http://www.baltimoresun.com/news/maryland/politics/bs-md-chelsea-manning-senate-20180213-story.html

Hansen, Evan. 2011. "Manning-Lamo chat logs revealed." *Wired*, July 13, 2011. https://www.wired.com/2011/07/manning-lamo-logs/

Heller, Nathan. 2017. "Chelsea Manning changed the course of history. Now she's focusing on herself." *Vogue*, August 10, 2017. https://www.vogue.com/article/chelsea-manning-vogue-interview-september-issue-2017

Ingber, Sasha. 2019. "Chelsea Manning Sent back to jail for refusing to testify before grand jury." National Public Radio, May 17, 2019. https://www.npr.org/2019/05/17/724133556/chelsea-manning-sent-back-to-jail-for-refusing-to-testify-before-grand-jury

Jones, Brian, and Paul Szoldra. 2017. "Chelsea Manning was just released from prison—Here's what happened during her trial." *Business Insider*, May 17, 2017. https://www.businessinsider.com/what-happened-in-chelsea-manning-trial-2017-5

Kelley, Michael B. 2013. "Bradley Manning acquitted of 'aiding the enemy,' convicted of 19 counts including espionage." *Business Insider*, July 30, 2013. https://www.businessinsider.com/bradley-manning-acquitted-of-aiding-the-enemy-2013-7

Pilkington, Ed. 2013. "Bradley Manning pleads guilty to 10 charges but denies 'aiding the enemy.'" *The Guardian*, February 28, 2013. https://www.theguardian.com/world/2013/feb/28/bradley-manning-pleads-aiding-enemy-trial

Savage, Charlie. 2017. "Chelsea Manning to be released early as Obama commutes sentence." *New York Times*, January 17, 2017. https://www.nytimes.com/2017/01/17/us/politics/obama-commutes-bulk-of-chelsea-mannings-sentence.html

Selk, Avi. 2017. "Chelsea Manning denies betraying the U.S., feels as if she lives in a 'dystopian novel.'" *The Washington Post*, September 18, 2017. https://www.washingtonpost.com/news/checkpoint/wp/2017/09/18/chelsea-manning-denies-betraying-the-u-s-feels-like-she-lives-in-a-dystopian-novel/?utm_term=.7b55e62c9c70

Shaer, Matthew. 2017. "The long, lonely road of Chelsea Manning." *New York Times*, June 12, 2017. https://www.nytimes.com/2017/06/12/magazine/the-long-lonely-road-of-chelsea-manning.html

United States Department of Justice. 2019. "WikiLeaks founder Julian Assange charged in 18-count superseding indictment." May 23, 2019. https://www.justice.gov/opa/pr/wikileaks-founder-julian-assange-charged-18-count-superseding-indictment

Valencia, Nick. 2010. "Berkeley tables resolution to call suspected WikiLeaks soldier 'hero.'" CNN, December 15, 2010. http://www.cnn.com/2010/US/12/15/california.berkeley.wikileaks/index.html

WikiLeaks. 2010. "Collateral murder." https://collateralmurder.wikileaks.org/en/index.html

MASTERS OF DECEPTION

The Masters of Deception were a gang of hackers and phreakers based primarily out of New York City in the late 1980s and early 1990s. It was started around June 1989, following the expulsion of Mark Abene (known online as Phiber Optik) from the Legion of Doom—another gang of hackers that existed at the time. Abene, along with Paul Sitra (known online as Scorpion) and Eli Ladopoulos (known online as Acid Phreak), were among those initially in the gang. Ladopoulos came up with the acronym for the name of the gang—MOD. This was a play on the acronym for the Legion of Doom (LOD). Ladopoulos chose the acronym as a way of trolling the Legion of Doom, noting that the letter "M" was the next step in the alphabet from the letter "L," and thus MOD were the next step in hacking from the Legion of Doom (LOD). The name "Masters of Deception" was chosen to fit that acronym later on (Slatalla and Quittner, 1995).

Although there may have been some animosity between the Masters of Deception and the Legion of Doom when the former was first formed, it was a later event that appears to have ignited the rivalry between the two groups. While online, a member of LOD called a member of MOD a racial slur. That MOD member was John Lee (known online as Corrupt), who was black. Additionally, Chris Goggans, a member of LOD, obtained a document of MOD's known as "The History of MOD" and used a filter to rewrite the document in "jive." This was seen as an additional race-based attack against Lee. Lee and others retaliated against Goggans and his newly-started cyber security firm, Comsec Data Security (Slattalla and Quittner, 1995; Tabor and Ramirez, 1992). The retaliation came in the form of overloading Comsec's phone lines with phone calls, and eavesdropping conversations on Comsec's phone lines (Slattalla and Quittner, 1995).

In 1992, five members of MOD where indicted by a federal grand jury for various computer crimes. The charges included unauthorized access to computers, unauthorized use of phone lines and long-distance calling card numbers, and interception of login credentials. Those indicted were Abene (20 years old), Sitra, Ladopoulos, Lee, and Julio Fernandez (18 years old, known online as Outlaw). Lee and Fernandez faced additional charges for selling login credentials that the purchasers used to gain unauthorized access to the credit reports of others (Tabor and Ramirez, 1992). Others in MOD had used login credentials to gain unauthorized access to the credit reports of others. Many of the reports pulled were of celebrities, including Geraldo Rivera, David Duke, John Gotti, Julia Roberts, Winona Ryder, Christina Applegate, and William Gaines. In one incident, Abene allegedly responded to a journalist calling him a "punk" online by pulling that journalist's credit report and displaying it to the journalist online (Slattalla and Quittner, 1995; Tabor and Ramirez, 1992). Only Lee and Ramirez, however, were alleged to have sold access to those credit histories.

All five ultimately pleaded guilty. Sitra (22 years old) and Ladopoulos (22 years old) were sentenced to six months of incarceration, followed by six months of house arrest. Lee (21 years old) was sentenced to a year in jail that was to be followed by three years of supervised release. While on supervised release, Lee violated the terms of his release by—among other things—acting as an accessory in an instance of wire communication interception. He was sentenced to an additional year of incarceration due to this violation of his release terms (*United States v. Lee*, 107 F.3d 4 (1997)). Abene was sentenced to a year in prison. Fernandez received a suspended sentence, apparently for his willingness to testify against his codefendants, though the need never arose (Slattalla and Quittner, 1995).

Following their sentences, several of these MOD members went on to work in the computer industry. Abene worked in network security from the early 2000's to at least 2015 (Bukszpan, 2015). Ladopoulos did computer work for a broadcasting company in New York following his release (Slattalla and Quittner, 1995). In 2015, he ran a security firm called Supermassive Corp. (Halime, 2015). Sitra worked with computers following his release, working for a business known as the Missing Person's Bureau (Slattalla and Quittner, 1995).

See also: Abene, Mark; Hacker and Hacking; Legion of Doom; Phreaker

Further Reading

Bukszpan, Daniel. 2015. "6 notorious hackers and their second careers." *Fortune*, March 18, 2015. https://fortune.com/2015/03/18/famous-hackers-jobs/

Halime, Farrah. 2015. "Hacker-proof helpers." *USA Today*, February 4, 2015. https://www.usatoday.com/story/tech/personal/2015/02/04/ozy-hacker-proof-helpers/22829861/

Slatalla, Michelle, and Joshua Quittner. 1995. *Masters of deception: The gang that ruled cyberspace*. New York: HarperCollins.

Tabor, Mary B. W., and Anthony Ramirez. 1992. "Computer savvy, with an attitude; Young working-class hackers accused of high-tech crime." *New York Times*, July 23, 1992. https://www.nytimes.com/1992/07/23/nyregion/computer-savvy-with-attitude-young-working-class-hackers-accused-high-tech-crime.html

MELISSA WORM

The Melissa worm—sometimes referred to as the Melissa virus—was a virus that was released on March 26, 1999. It was designed by David Lee Smith. The virus was apparently named after a stripper that Smith knew from Florida (Cluley, 2009; Federal Bureau of Investigation, 2019). The virus spread through the use of infected attachments in e-mails. It is one of the first viruses—if not the first virus—to utilize mass e-mailing to spread (Cluley, 2009; Long, 2010).

The virus originated from Microsoft Word document uploaded by Smith to a Usenet discussion group called alt.sex. The document purported to be a list of 80 free passwords to pornographic websites (Federal Bureau of Investigation, 2019; Long, 2010). Once the document was opened, the virus would hijack the user's Microsoft Outlook software and send out e-mails to the first 50 people in the user's e-mail address book (Cluley, 2009; Federal Bureau of Investigation, 2019). The e-mails contained an attachment, and would include language to encourage e-mail recipients to open the attachment. Apparently trying to appeal to the same curiosities as the initial document on the alt.sex forum did, e-mail attachments would have names such as "naked wife" and "sexxxy.jpg." Other e-mails would include a message in the body of the e-mail claiming that the attachment was something the recipient had requested, and that they should not show the attachment to anyone else (Federal Bureau of Investigation, 2019). If a recipient opened the attachment, the process would repeat, sending e-mails with virus-laden attachments to the first 50 people in the recipient's e-mail address book. In this way, the virus spread exponentially.

Investigators were able to trace the virus back to the initial document posted on the alt.sex forum. The document had been uploaded by an America Online (AOL) user known as skyrocket@aol.com. However, investigators determined that account had been compromised by a hacker, which they later determined to be Smith (Cluley, 2009). Smith, who went by the online name of Kwijybo (a term from the television show *The Simpsons*), was also determined to be the author of the virus (Cluley, 2009; Long, 2010). Smith was arrested at his residence in New Jersey on April 1, 1999 (Federal Bureau of Investigation, 2019).

Smith does not appear to have been financially motivated in his design of the Melissa worm. To the investigators' understanding, it was designed to show he could do it (Cluley, 2009). Nonetheless, the virus did have a financial impact. Where the virus spread exponentially, e-mail servers became clogged, impairing the functionality of the servers. It is estimated that it cost victims $80 million to repair the damage done by the Melissa virus (Federal Bureau of Investigation, 2019).

Following his arrest, Smith agreed to cooperate with law enforcement. He pleaded guilty to charges against him in December, 1999 (Federal Bureau of Investigation, 2019). He assisted the FBI with other cybercrime investigations. He provided contact information for Jan de Wit—the designer of the Anna Kournikova virus—which led to de Wit's arrest in the Netherlands. It is believed that Smith also assisted the FBI with an investigation into virus author Simon Vallor, who was ultimately arrested in the United Kingdom in 2001 (Cluley, 2009). Smith was sentenced in May 2002 to 20 months in prison for his crimes (Federal Bureau of Investigation, 2019).

See also: Virus; Worm

Further Reading

Cluley, Graham. 2009. "Memories of the Melissa virus." Sophos, March 26, 2009. https://nakedsecurity.sophos.com/2009/03/26/memories-melissa-virus/

Federal Bureau of Investigation. 2019. "The Melissa virus." March 25, 2019. https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519

Long, Tony. 2010. "March 26, 1999: 'Melissa' wreaks havoc on net." *Wired*, March 26, 2010. https://www.wired.com/2010/03/0326melissa-worm-havoc/

MITNICK, KEVIN (1963–)

Kevin Mitnick became one of the world's most known hackers and is now known as the world's leading authority on hacking. Once known as the world's most wanted hacker, Mitnick now uses the same skills that once put him into prison to help companies and individuals stay safe when using the internet.

Mitnick was born in California in 1963 and grew up in Los Angeles during the 1970s. He became an amateur radio operator during high school. He had a natural curiosity about how things worked, which led him to becoming one of the most famous members of hacker culture.

At the age of 13, Mitnick used dumpster diving and social engineering to obtain a free public bus pass. When he was 16, Mitnick learned how to "phone phreak" and make calls for free. He and some friends entered the offices of PacBell (the phone company) after business hours and stole various documents and manuals that pertained to the inner workings of the phone system. A girlfriend of one of the other men told the LA district attorney about the break-in, and Kevin was arrested. Because he was a juvenile offender, Mitnick was sentenced to a diagnostic study and placed on probation for one year.

Despite his criminal activities, Mitnick attended Pierce College and University of Southern California, where he studied computers. While at USC, he identified a vulnerability in the school's computers and gave himself full administrative privileges. When caught, school administrators allowed him to remain as a student in the school on the stipulation the he finish a project as a punishment. The topic of that project was to increase the security of the school's computers.

In 1982, it was reported that Mitnick hacked into the computer system at the North American Aerospace Defense Command (NORAD), which became the basis of the movie *WarGames* (1983). This is an allegation Mitnick denies. He also denies allegations that he hacked into the network of the FBI.

Mitnick admits that he tapped into the computers at Pacific Bell, where he tapped phone lines and accessed unlisted phone numbers. In the end, he had control of the company's entire network. He was also able to break into the computer network of the Digital Equipment Corporation and copied their software. When he recognized that he was under investigation for these actions, Mitnick wiretapped the agents who were looking into his actions. He was able to create an early warning system that would warn him if the agents were planning to raid his home. On the day the FBI came to arrest him, Mitnick had cleared his apartment of any evidence and placed a box of "FBI Donuts" out for the agents.

To avoid arrest, Mitnick went on the lam from law enforcement. For two years Mitnick hid from agents. During his time on the run, he was in Denver, Colorado, living under the name Eric Weiss (Harry Houdini's real name). He worked with computer security for a law firm, Holme Roberts & Owen. He also spent time working in a hospital in Seattle where he was known as Brian Merril. Throughout, Mitnick continued to access networks, making modifications to the systems, reading e-mails, and copying software. He was put on the FBI's most wanted hacker list. He had lost weight, so his appearance was not as pictured by the agency.

During this time, Mitnick continued to hack into different networks, stealing proprietary software from cell phone companies, including Motorola, Nokia, and Sun. He also stole passwords, read private e-mails, and modified networks. He used social engineering techniques to gather usernames and passwords from people.

Mitnick was arrested again in February 1995, in North Carolina. He was accused of hacking into a computer of a research scientist named Tsutomo Schiomura, who was able to trace the hack back to Mitnick. He was charged with unauthorized access to a federal computer and 14 counts of wire fraud. He was also charged with eight counts of possessing unauthorized access devices, interception of wire or electronic communications, unauthorized access to a federal computer, and causing damage to a computer. In exchange for pleading guilty to four counts of wire fraud, two counts of computer fraud, and one count of illegal intercepting a wire communication, Mitnick was sentenced to 46 months in prison, with an additional 22 months for violating his supervised release by hacking into Pacific Bell.

Mitnick spent five years in prison on these charges. Four and a half of those were before the trial. Prison officials forced him to eight months in solitary confinement because they considered him to be a threat and claimed he could start a nuclear war by whistling into a pay phone or by hacking into the NORAD system. He was released in January, 2000, and given three years of probation, serving on supervised release until January 2003. He was prohibited from using technology with the exception being a land line phone. Mitnick appealed the decision and was allowed to use the internet. He was also prohibited from profiting from his story.

In December 2002, a judge declared that Mitnick was rehabilitated enough to be given an amateur radio license. He has appeared as a computer security expert on many television shows (*60 Minutes*, Court TV, *Good Morning America*, CNN, National Public Radio) and has been the focus of magazine articles and newspaper stories. He now runs a computer security company, Mitnick Security Consulting LLC. He will examine a company's computer systems for weaknesses and vulnerabilities. He also advises the FBI and other Fortune 500 companies.

Mitnick has also become an author, penning *The Art of Invisibility*; *Ghost in the Wires*; and *The Art of the Deception*. He appeared on an episode of the television show "Alias" as a hacker. He also goes on speaking tours to tell his story and talk about security issues. Congress sought out his expertise and asked him to testify about the state of cybercrime and the need for additional laws. In his written testimony, Mitnick declared, "I have gained unauthorized access to computer systems at some of the largest corporations on the planet, and have successfully penetrated some of the most resilient computer systems ever developed" (Testimony for the U.S. Senate Governmental Affairs Committee, March 2000). Despite this, he considers himself to be a recreational hacker who never sold any information for profit or personal gain. He never stole money from another person or anyone's identity. He simply enjoys the challenge of hacking a system to see how it works (Penenberg, 1999).

See also: Engressia, Josef Carl, Jr.; Hacker and Hacking; White-Hat Hackers

Further Reading

Chuang, Tamara. 2018. "Kevin Mitnick was the FBI's most wanted hacker in the 90s. He was hiding in plain sight in Denver." *Denver Post*, March 16, 2018. https://www.denvepost.com/2018/03/16/kevin-mitnick-fbi-most-wanted-hacker-denver/

"A convicted hacker debunks some myths." CNN, October 13, 2005. http://www.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/

Green, Andy. 2014. "Kevin Mitnick, once the world's most wanted hacker, is now seeing zero-day exploits." *Security*, September 24, 2014. https://www.wired.com/2014/09/kevin-mitnick-selling-zero-day-exploits/

Hafner, Katie, and John Markoff. 1991. *Cyberpunk: Outlaws and hackers on the computer frontier*. New York: Simon & Schuster.

Mitnick, K. D., and W. L. Simon. 2002. *The art of deception: Controlling the human element of security*. New York: Wiley Publishing.

Mitnick, K. D., and W. L. Simon. 2005. *The art of intrusion*. Indianapolis, IN: Wiley.

Penenberg, Adam L. 1999. "Mitnick speaks!" *Forbes*, April 5, 1999. https://www.forbes.com/1999/04/05/feat.html#36d2a97a6d8d

Shimomura, Tsutomu, and John Markoff. 1996. *Take-down: The pursuit and capture of Kevin Mitnick, America's most wanted computer outlaw*. New York: Hyperion.

MONEY LAUNDERING

Money laundering is the process of filtering the proceeds of illegal activity through seemingly-legitimate sources (e.g., bank accounts, businesses) to obfuscate the true origin of those funds. Money laundering is common in drug trafficking and other organized crime. While money can be laundered through noncyber means, there are cyber methods through which money can be laundered as well. Money laundering occurs to enable criminals to make use of the proceeds of their crimes without arousing law enforcement suspicion.

Any method that can hide the true origin of money and allow the criminal to use those funds without suspicion can be used. Foreign bank accounts and money services might be used to hide the origins of the funds. In one case investigated by the U.S. Drug Enforcement Administration (DEA) and Internal Revenue Service (IRS), it was found that drug cartels were using money exchange houses in Mexico to purchase drug trafficking equipment in the United States (Vulliamy, 2011). Those exchange houses were able to use fake identities, and send funds to the United States through Wachovia bank to make these purchases. The investigation discovered that over $378 billion was likely laundered through Wachovia. Wachovia bank was criminally charged for its failure to have a system in place to prevent the bank from being used to launder money. Although the bank itself was criminally charged, none of its executives were. It ultimately was required to pay $160 million to the United States as part of an agreement entered between the bank and the government (Vulliamy, 2011).

Cyber methods have been increasingly used to launder money. Cyber money laundering employs similar techniques as noncyber money laundering. In the case of Wachovia bank, the key thing money launderers sought to do was anonymize the monetary transactions—something they were able to accomplish through the use of exchange houses in Mexico. With cyber money laundering, the use of a cryptocurrency or other digital currency can accomplish this. To do this, money launderers will first convert their cash into a digital currency. Bitcoin is perhaps the most well-known cryptocurrency. However, Bitcoin is not truly anonymous. What makes Bitcoin work is its use of blockchains—public ledgers of all Bitcoin transactions that take place. Thus, not only is there a record of all transactions, but it is publicly available to everyone, including law enforcement. If law enforcement has a monitoring tool that enables them to tie a person to an initial Bitcoin transaction, tracing the money is easy at that point (Bloomberg, 2017). Because of this, cybercriminals have turned to other cryptocurrencies—sometimes referred to as altcoins—to launder money. Specifically, a cybercriminal might use a category of altcoin referred to as privacy coins—cryptocurrencies that afford their users anonymity when conducting transactions. After a cybercriminal converts funds to Bitcoin, a cybercriminal can use a service that "mixes" Bitcoins. These services attempt to use temporary Bitcoin wallets to route Bitcoin through. When those temporary wallets are no longer available, the hope is the Bitcoin will no longer be traceable. From there, the Bitcoin can be converted to a privacy coin. A launderer may convert the initial Bitcoin to several different privacy coins. From there, a launderer can convert those anonymous privacy coins back into Bitcoin and, from there, back into standard currency. At that point, the origin of the funds will have been thoroughly obfuscated (Fruth, 2018).

There have been cases of cyber money laundering involving significant amounts of money. In 2013, U.S. authorities shut down Liberty Reserve—an online money transfer business—for laundering $6 billion. Executives of the company were arrested. At the time of its shut down, Liberty Reserve had roughly 1,000,000 customers around the world, 200,000 of those residing in the United States. The company permitted customers to create accounts without verifying their identities. This permitted customers to create accounts using fake identifying information (Isodore, 2013). Liberty Reserve operated using a digital currency known as LR. Payments could be made to other Liberty Reserve customers using LR. Liberty Reserve did not permit customers to directly fund their accounts from other outside personal accounts. Rather, customers had to go through specific third-party exchange companies that would process deposits and withdrawals. This further allowed Liberty Reserve to not collect any personally identifying information on its customers. In addition to this, customers submitting payments could opt to pay a privacy fee (75 cents) to remove reference to the customer's account number from transfer of LR. This made LR transactions untraceable, even by Liberty Reserve itself (Mabunda, 2018). All these procedures afforded customers a significant amount of anonymity with their financial transactions. Accordingly, many cybercriminals used the site to facilitate criminal activity or hide the proceeds of criminal activity, such as drug trafficking, credit card fraud, and Ponzi schemes (Isodore, 2013; United States Department of Justice, 2016). The founder of Liberty Reserve (Arthur Budovsky) pleaded guilty to conspiracy to commit money laundering. On May 6, 2016, he was sentenced to 20 years in prison and received a $500,000 fine (United States Department of Justice, 2016).

Another cyber money launderer was arrested in 2017. Alexander Vinnik—a Russian national—was arrested in Greece for laundering money through BTC-e, a Bitcoin exchange operated by him. It is alleged that Vinnik used BTC-e to facilitate crimes such as drug trafficking, identity theft, and fraud. It is believed that Vinnik laundered $4 billion. It is also believed Vinnik obtained funds that had been hacked from the Bitcoin exchange Mt. Gox in 2014 (Artois, 2017). As of early 2019, Vinnik's case is still pending. He is currently still in custody in Greece. The United States has sought to have him extradited, as have France and Russia, who also have charges pending against him (Alexandre, 2019).

See also: Bitcoin; Cryptocurrency; Digital Currency; Drug Trafficking

Further Reading

Alexandre, Ana. 2019. "Russian official seeks extradition of alleged Bitcoin fraudster Alexander Vinnik." *Coin Telegraph*, February 25, 2019. https://cointelegraph.com/news/russian-official-seeks-extradition-of-alleged-bitcoin-fraudster-alexander-vinnik

Artois, Stella. 2017. "Cyber criminal who laundered £3bn in bitcoin arrested in Greece." *The Telegraph*, July 27, 2017. https://www.telegraph.co.uk/technology/2017/07/27/cyber-criminal-laundered-3bn-bitcoin-arrested-greece/

Bloomberg, Jason. 2017. "Using Bitcoin or other cryptocurrency to commit crimes? Law enforcement is onto you." *Forbes*, December 28, 2017. https://www.forbes.com/sites/jasonbloomberg/2017/12/28/using-bitcoin-or-other-cryptocurrency-to-commit-crimes-law-enforcement-is-onto-you/#45db9643bdc4

Fruth, Joshua. 2018. "'Crypto-cleansing': Strategies to fight digital currency money laundering and sanctions evasion." *Reuters*, February 13, 2018. https://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-cleansing-strategies-to-fight-digital-currency-money-laundering-and-sanctions-evasion-idUSKCN1FX29I

Isodore, Christopher Violante. 2013. "Arrests made in $6 billion cyber money-laundering case." CNN, May 28, 2013. https://money.cnn.com/2013/05/28/news/companies/money-laundering-arrests/index.html

Mabunda, Sagwadi. 2018. "Cryptocurrency: The new face of cyber money laundering." *International Conference on Advances in Big Data, Computing and Data Communication Systems*. IEEE, August 6–7, Durban, South Africa.

United States Department of Justice. 2016. "Liberty Reserve founder sentenced to 20 years for laundering hundreds of millions of dollars." May 6, 2016. https://www.justice.gov/opa/pr/liberty-reserve-founder-sentenced-20-years-laundering-hundreds-millions-dollars

Vulliamy, Ed. 2011. "How a big US bank laundered billions from Mexico's murderous drug gangs." *The Observer*, April 2, 2011. https://www.theguardian.com/world/2011/apr/03/us-bank-mexico-drug-gangs

MORRIS, ROBERT TAPPAN (1965–)

Robert Morris was born on November 8, 1965, the son of a computer scientist at Bell Labs and later the chief scientist at the National Computer Security Center (part of the National Security Agency). Morris went to Harvard University and then to Cornell University for graduate school. While there, he sought to learn more about the security of computer systems. He wrote what became the first computer worm, aptly named the Morris worm. He was 21 years old when the worm was released on November 2, 1988. The worm spread quickly through the internet, marking the first time the internet was attacked.

The Morris worm was a self-replicating program that copied itself and then infected machines much more quickly than Morris intended. It was estimated that the worm infected about 6,000 computers in a 12-hour span. The malware affected computers all around the country—in universities, medical facilities, and the military. An infected machine would slow down to the point that they were unusable, or would simply crash. Because the worms infected so many computers, it brought portions of the internet to a standstill. When Morris realized the potential harm he had caused, he attempted to solve the problem. However, it was difficult to discover if a computer had been infected, and it was even more difficult to stop it from spreading.

At first, Morris tried to contact the system administrators at Cornell University, but they were unable to stop the virus from spreading. Morris and a friend devised a method to kill the worm and tried to send an e-mail over the internet, but because the network was clogged, the message didn't reach users. Other solutions were devised by computer experts at Purdue University and at the University of California at Berkeley.

Morris had no intention to cause any damage or the resulting panic. The only purpose was to break into as many computers as he could. The damages from the attack were estimated to be around $100 million. Despite his lack of malevolent intent, Morris was indicted for violating the Computer Fraud and Abuse Act of 1986. He was the first person to be indicted under the new law. He was sentenced to three years of probation, with 400 hours of community service, and a fine of $10,000. Morris appealed the conviction, but the appeal was not successful.

In the end, Morris received a PhD from Harvard, became a tenured faculty member at the Massachusetts Institute of Technology, and is a co-founder of Viaweb, a software company that helps people with few technical skills create an online store by using a web browser. The worm he wrote brought the vulnerability of the internet to the public's attention for the first time. People realized that the internet was not secure and that it wasn't possible to rely on other users' good intentions to police themselves. Instead, the dangers of the internet became clearer.

See also: Malware; Worm

Further Reading

Fuchs, Erin. 2013. "How the 'Computer Wizard' who created the first internet virus got off without a day of jail." *Business Insider*, January 21, 2013. https://www.businessinsider.com/why-robert-morris-didnt-go-to-jail-2013-1

Kehoe, Brendan P. 1996. *Zen and the art of the internet: A beginner's guide.* Upper Saddle River, NJ: Prentice Hall.

Lee, Timothy B. 2013. "How a grad student trying to build the first botnet brought the internet to its knees." *Washington Post*, November 1, 2013. https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/?noredirect=on&utm_term=.b88af037afff.

Markoff, John. 1988. "Author of computer 'virus' is son of N.S.A. expert on data security." *New York Times*, November 5, 1988. https://www.nytimes.com/1988/11/05/us/author-of-computer-virus-is-son-of-nsa-expert-on-data-security.html

Middleton, Bruce. 2017. *A history of cyber security attacks: 1980 to present*. Boca Raton, FL: CRC Press.

MOTIVES

There are several reasons why a person may decide to commit cybercrime. Several typologies of cybercriminal motivation have been suggested (Li, 2017). There are commonalities between these typologies. Coupled with statistics on cybercriminal motivations, this data suggests some common motivations of cybercriminals. One's motivations for committing cybercrime may have an impact on what type of cybercrime that person commits, and the manner they choose to commit it in.

The most prevalent motivation for people to commit cybercrime appears to be financial gain. One report on data breaches found that 71 percent of those breaches were perpetrated for the purpose of financial gain (Verizon, 2019). Based on complaints made to the FBI, victims of cybercrime lost $1.42 billion in 2017 (Federal Bureau of Investigation, 2018). The financial gain can come in the form of income received, as would happen in instances of credit card fraud, instances where ransomware is used, and instances where financial institutions have their network compromised. Financial gain can also come in the form of payment avoided for goods or services. Intellectual property theft is perhaps the most prevalent example of this type of financial gain. Estimates show that the annual amount lost to intellectual property theft by intellectual property owners in the United States is between $225 and $600 (Commission on the Theft of American Intellectual Property, 2017).

The second most prevalent motivation for people to commit cybercrime appears to be espionage. The same report that found 71 percent of data breaches to be financially motivated also found that 25 percent of data breaches were perpetrated as espionage (Verizon, 2019). Espionage appears to be the motive of cybercriminals acting at the behest of a country (Ablon, 2018). Examples of this can be seen in China.

In 2015, it was discovered that the People's Liberation Army (PLA) covertly installed microchips in servers made in China that permitted China to surreptitiously monitor activity on those servers and gather information from those servers. Those servers were used by various foreign businesses and government agencies (Robertson and Riley, 2018). In 2017, China Aerospace Science and Industry Corporation sold biometric hardware to Taiwan that similarly allowed employees of the state-owned business to surreptitiously gather information on who was leaving and entering Taiwan (Center for Strategic and International Studies, 2019).

Another potential motivation for cybercriminals is retaliation. Revenge porn—the posting of sexually explicit pictures or video of another person with that person's consent—is a cybercrime that is often perpetrated for this reason. This occurs when a former romantic partner posts sexually explicit pictures of someone following a breakup. The use of a logic bomb can also be used for retaliatory purposes. In some instances, disgruntled employees may install a logic bomb on the computer network of their employer. That logic bomb can be programmed to delete software and computer files from the employer's computer network if the employee is ever fired (Armendariz, 2019). Any type of cyberattack, however, can be perpetrated as a form of retaliation. An example of this is the attacks on Sony Pictures by North Korea in 2014. The attack destroyed data on Sony's network. North Korea also stole information from Sony as part of the attack. It appears the attack was carried out by North Korea due to Sony's upcoming release of the movie *The Interview*. The movie's plot centered on the protagonists assassinating North Korean president Kim Jong-un (Chanlett-Avery et al., 2017).

Some cybercrimes are committed for ideological reasons. This would include crimes committed by hacktivists. Hacktivists often use DDoS attacks and disseminations of private information as part of their attacks (Ablon, 2018). For example, the hacktivist group Anonymous has used DDoS attacks against the websites of several entities it disagrees with, including the Vatican, the Church of Scientology, and child pornography websites (Cuthbertson, 2017; McMillan, 2008; Protalinski, 2012). Another group known as the Impact Team stole customer information from Ashley Madison—a website designed to facilitate marital affairs—and released that information online. This was done because the Impact Team felt the business practices of Ashley Madison—namely, retaining customer information despite promising not to do so—were dishonest (Thomsen, 2015).

Hacktivism has been in decline. Between 2015 and 2019, hacktivist incidents dropped 95 percent (Cimpanu, 2019). There are other entities that engage in cybercrime for ideological reasons. There are a number of groups engaged in politically based cyberattacks. Some of these groups are part of a government or state-sponsored, such as the PLA in China and the Russian Main Intelligence Directorate (GRU). Others act independently of a country, even though their actions may be approved of by that government. This can be seen with the Syrian Electronic Army. The ideology supported by these cyber groups can vary, though they will generally engage in attacks that support the government that sponsors them, or possibly work against governments they oppose if they are not sponsored by those governments. Another potential group of cybercriminals with ideological motivations is white hat hackers. White hat hackers are hackers that hack into computer networks to expose flaws in the system and then report those flaws to the owner of the network. Their ideological motivation is to make the internet a more secure place. White hat hacking can be legal is done with the permission of owner of the network. However, even though there is a benefit to the entities who receive a list of flaws in their network, a white hat hacker is potentially acting illegally if they hack a network without permission.

Some people may commit cybercrime because they find it entertaining. Those people may find the challenge of hacking thrilling. They may do it for recognition from their peers, or simply because they are curious about how hacking works (Li, 2017). This sentiment is captured in an essay called "The Conscience of a Hacker":

> We explore . . . and you call us criminals. We seek after knowledge . . . and you call us criminals. We exist without skin color, without nationality, without religious bias . . . and you call us criminals. . . . Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for. (The Mentor, 1986)

There are specific cybercrimes that may be committed for voyeuristic reasons. These crimes exist outside the cyber realm, though have certainly become common online criminal activities. Examples of this are the possession of child pornography and stalking.

There can be multiple motivations to commit any one given cybercrime. The crime of sextortion—threatening to release sexually explicit pictures or video of someone unless they agree to pay the perpetrator—has a clear financial motive, but the crime often has a retaliatory motive as well; as with revenge porn, sextortion often occurs between former romantic partners who have since separated. Likewise, attacks carried out by state-sponsored hacking groups have multiple motives. North Korea's attack on Sony Pictures had a retaliatory motive as was noted above, but there is also an ideological political motive as the attack appears to have been committed to attack the idea of assassinating the leader of North Korea. The same can be said of the PLA covertly installing microchips on motherboards manufactured in China. The purpose of installing the microchips was espionage, but that espionage is also committed for political reasons—advancing the strategic interests of China.

See also: Black-Hat Hackers; Child Pornography; China; Copyright Infringement; Credit Card Fraud; Distributed Denial-of-Service Attack (DDoS); Federal Bureau of Investigation; Financial Crimes; Hacktivism; People's Liberation Army Unit 61398; Political Uses; Ransomware; Revenge Porn; Syrian Electronic Army; White-Hat Hackers

Further Reading

Ablon, Lillian. 2018. "Data thieves: The motivations of cyber threat actors and their use and monetization of stolen data." Rand Corporation, March 15, 2018. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf

Armendariz, Tommy. 2019. "What is a logic bomb?" Lifewire, March 4, 2019. https://www.lifewire.com/what-is-a-logic-bomb-153072

Center for Strategic and International Studies. 2019. "Significant cyber incidents." https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

Chanlett-Avery, Emma, Liana W. Rosen, John W. Rollins, and Catherine A. Theohary. 2017. "North Korean cyber capabilities: In brief." Congressional Research Service, August 3, 2017. https://fas.org/sgp/crs/row/R44912.pdf

Cimpanu, Catalin. 2019. "Hacktivist attacks dropped by 95% since 2015." *ZDNet*, May 17, 2019. https://www.zdnet.com/article/hacktivist-attacks-dropped-by-95-since-2015/

Commission on the Theft of American Intellectual Property. 2017. "Update to the IP Commission Report." http://ipcommission.org/report/IP_Commission_Report_ Update_2017.pdf

Cuthbertson, Anthony. 2017. "Anonymous hacker takes down 20 percent of dark web in child porn operation." *Newsweek*, February 6, 2017. https://www.newsweek.com/anonymous-hacker-dark-web-child-porn-operation-553014

Federal Bureau of Investigation. 2018. "2017 internet crime report." Federal Bureau of Investigation. https://pdf.ic3.gov/2017_IC3Report.pdf

Li, Xingan. 2017. "A review of motivations of illegal cyber activities." *Criminology & Social Integration Journal* 25, 1: 110–126.

McMillan, Robert. 2008. "Hackers hit Scientology with online attack." *PCWorld*, January 26, 2008. https://www.pcworld.com/article/141839/article.html

The Mentor. 1986. "The conscience of a hacker." *Phrack* 1, 7. http://www.phrack.org/issues/7/3.html

Protalinski, Emil. 2012. "Anonymous hacks Vatican website." *ZDNet*, March 12, 2012. https://www.zdnet.com/article/anonymous-hacks-vatican-website/

Robertson, Jordan and Michael Riley. 2018. "The big hack: How China used a tiny chip to infiltrate U.S. companies." *Bloomberg Businessweek*, October 4, 2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Thomsen, Simon. 2015. "Extramarital affair website Ashley Madison has been hacked and attackers are threatening to leak data online." *Business Insider*, July 20, 2015. https://www.businessinsider.com/cheating-affair-website-ashley-madison-hacked-user-data-leaked-2015-7

Verizon. 2019. "2019 data breach investigations report." https://enterprise.verizon.com/resources/reports/dbir/2019/introduction/

MPACK

MPack is malware that was designed in 2006 by a group known as Dream Coders, which is primarily based out of Russia (Lemos, 2007). MPack is an exploit kit—malware designed to exploit vulnerabilities in software on targeted computers, most often in web browsers. Once the vulnerability is exploited, the exploit kit can download further malware on the compromised computer. MPack is the first known instance of an exploit kit (Malwarebytes, 2016).

Despite the fact that the use of exploit kits is illegal, they are often treated like a piece of commercial software. This can include technical support for customers and software updates for the exploit kit (Malwarebytes, 2016). MPack did this. When it was first released, Dream Coders sold MPack for between $500 and $1,000, and the purchase came with one year of technical support from Dream Coders (Lemos, 2007; Leyden, 2007).

MPack is designed to be installed on a server, and then exploit vulnerabilities in the web browsers connecting to that server. Malicious code known as iframe is used to direct traffic to an MPack server (Lau, 2007; Leyden, 2007). Various methods can be used to cause a target web browser to run the iframe code, such as including the code in spam e-mails, including the code in typosquatted websites, or hacking into legitimate websites and embedding the code into those websites (Lau, 2007). In some instances where legitimate websites were hacked and the iframe code embedded in them, other websites hosted on that same server were also infected with the code. This occurred where the servers hosting those websites were improperly configured (Leyden, 2007). Once a web browser connects to the server on which MPack is installed, MPack determines what web browser is being used and deploys the exploit corresponding to that browser, enabling the computer using that browser to be compromised. Once compromised, further malware is downloaded to the computer (Lau, 2007).

MPack appears to have been a popular exploit kit for cybercriminals to use. In 2010, one report found that two-thirds of malicious activity online was brought about through the use of exploit kits and other tool kits. MPack was found to be the most used tool kit, with 48 percent of the tool kits being used being MPack. It is suspected that the ease with which cybercriminals could access tool kits like MPack contributed to the increase in cybercrime seen at the time of the report (Messmer, 2011). As of 2019, it appears that exploit kits are still popular with cybercriminals (Chebyshev et al., 2019). However, MPack itself does not appear to be at the forefront of the antivirus community as it was for the first several years following its release.

See also: Cybersquatting; Hacker and Hacking; Malware; Russia; Spam

Further Reading

Chebyshev, Victor, Fedor Sinitsyn, Denis Parinov, Boris Larin, Oleg Kupreev, and Evgeny Lopatin. 2019. "IT threat evolution Q1 2019. Statistics." Kaspersky, May 23, 2019. https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/

Lau, Hon. 2007. "MPack, packed full of badness." Symantec, May 27, 2007. https://www.symantec.com/connect/blogs/mpack-packed-full-badness

Lemos, Robert. 2007. "Newsmaker: DCT, MPack developer." SecurityFocus, July 20, 2007. https://www.securityfocus.com/news/11476/1

Leyden, John. 2007. "MPack malware exposes cheapskate web hosts." *The Register*, July 3, 2007. https://www.theregister.co.uk/2007/07/03/mpack_reloaded/

Malwarebytes. 2016. "Exploit kits." Malwarebytes, June 9, 2016. https://blog.malwarebytes.com/threats/exploit-kits/

Messmer, Ellen. 2011. "MPack, NeoSploit and Zeus top most notorious Web attack toolkit list." NetworkWorld, January 18, 2011. https://www.networkworld.com/article/2198847/mpack--neosploit-and-zeus-top-most-notorious-web-attack-toolkit-list.html

N

NAKAMOTO, SATOSHI

Satoshi Nakamoto is the name claimed by the anonymous inventor of the cryptocurrency Bitcoin, the first such digital currency. Nakamoto published the original document explaining the Bitcoin system in 2008. Where Bitcoin are a digital currency, there is no tangible currency to actually hold. Nakamoto's invention of Bitcoin was the invention of the system by which a cryptocurrency like Bitcoin could exist. Specifically, it was the system of using blockchains—decentralized public strings of data entries that are tied one to another via cryptography—to track monetary transactions that made Bitcoin possible. Bitcoin are generated through a process known as mining—verifying the transactions in a blockchain. Those who mine are rewarded for mining with Bitcoin. In this way, Bitcoin becomes more widespread and established the more people use the cryptocurrency. After Nakamoto devised this system, all that needed to happen to get Bitcoin rolling was to start making Bitcoin transactions. The first Bitcoins were transferred the following year, from Nakamoto to Hal Finney (Bitcoin, 2018).

Nakamoto has guarded his anonymity zealously. He disappeared from public view in 2011, shortly after his disassociation from Bitcoin. Nakamoto never revealed his real-world identity, and there has been much speculation over Nakamoto's true identity (Chen, 2016). The name Satoshi Nakamoto is Japanese in origin, though given Nakamoto's ability to speak English perfectly in his online communications, many suspect that Nakamoto is not actually Japanese. Additionally, his use of British spellings of certain words in his communications and his Bitcoin source code notes have led people to believe Nakamoto to be British. However, other evidence compiled by Stefan Thomas—a coder from Switzerland who was active in the Bitcoin community—suggested that Nakamoto might live on the east coast of the United States. Stefan tracked the timestamps on all of Nakamoto's posts in Bitcoin forums and discovered that Nakamoto rarely if ever posted during what would be the nighttime (roughly midnight to 6:00 a.m.) on the east coast of the United States, leading to the belief that Nakamoto was not posting during those hours because he lived on the east coast and was asleep (Wallace, 2011).

Even those who worked closely with Nakamoto on Bitcoin did not gain any special insight into his true identity. Laszlo Hanyecz is one such person. Hanyecz is perhaps best known as the person to make the first real-world purchase using Bitcoin—two pizzas from Papa John's. Hanyecz corresponded regularly with Nakamoto via e-mail while working on Bitcoin—helping debug the Bitcoin code and so forth. Despite the regular communication, Nakamoto never divulged personal information to Hanyecz. Hanyecz has indicated that many of his communications with Nakamoto felt odd (Bernard, 2018b) and posited that at times it felt like Nakamoto was not in fact a single person (Wallace, 2011). Others have also speculated that Nakamoto might actually be a pseudonym for a group of people (L. S., 2015; Wallace, 2011).

There have been several individuals that people have speculated are Satoshi Nakamoto. *Newsweek* claimed to have found Nakamoto in 2014. There was a man by the name of Dorian Prentice Satoshi Nakamoto who lived in Temple City, California, who was a physicist who had done classified work for the U.S. military in the past. According to the report by *Newsweek*, Nakamoto said the following when asked about Bitcoin: "I am no longer involved in that and I cannot discuss it. It's been turned over to other people. They are in charge of it now. I no longer have any connection."

Nakamoto denies he is the Satoshi Nakamoto that created Bitcoin (Goodman, 2014). Several have claimed that Nick Szabo—a cryptographer and creator of the cryptocurrency bit gold in the 1990s—is really Nakamoto. Szabo has denied these claims as well (Bernard, 2018a; L. S., 2015). Hal Finney—the person who received the first Bitcoins in a transfer from Nakamoto—has been claimed by many to be Nakamoto as well. As with others, Finney denied this (Greenberg, 2014). There is one individual who did claim to be Nakamoto—an Australian businessman named Craig Wright. Wright made this claim in 2016 and indicated he would back up his claim with proof of access to early Bitcoin keys. However, he ultimately did not provide this proof, claiming he lacked the courage to disclose the proof amid the attention he received—from skeptics in the cryptocurrency community to the FBI—after making his claim to be Nakamoto (Bernard, 2018a).

While sleuthing the identity of Nakamoto may simply be entertaining for some, there is an argument that knowing the true identity of Nakamoto would be beneficial for the existence of Bitcoin. There have arisen (and potentially arise in the future) disputes among Bitcoin developers on how to handle emerging issues with the cryptocurrency, such as dealing with an increased user base. Having the actual creator of Bitcoin around to weigh in on these debates could provide a definitive resolution (Chen, 2016). Bitcoin itself has argued the opposite, stating that knowing the identity of Nakamoto is "probably as relevant today as the identity of the person who invented paper" (Bitcoin, 2018).

Nakamoto was involved with Bitcoin until 2010, at which point he separated from the company (Bitcoin, 2018). Nakamoto has rarely been heard from since. As with Nakamoto's true identity, the reason for Nakamoto's departure from Bitcoin are not clear. In one of the last known communications from Nakamoto on April 23, 2011, Nakamoto said the following in an e-mail in response to an inquiry from Mike Hearn—a Bitcoin developer—about his future involvement in Bitcoin: "I've moved on to other things. It's in good hands . . ." (Bernard, 2018a; Pearson, 2017). Even though Nakamoto did disassociate from Bitcoin, he did keep numerous Bitcoin after his departure. It is estimated that Nakamoto owns 980,000 Bitcoin, which would be worth over $17 billion based on Bitcoin values around the end of 2017 (Schroeder, 2017).

See also: Bitcoin; Cryptocurrency; Privacy

Further Reading

Bernard, Zoë. 2018a. "Everything you need to know about Bitcoin, its mysterious origins, and the many alleged identities of its creator." *Business Insider*, November 10, 2018. https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12

Bernard, Zoë. 2018b. "Satoshi Nakamoto was weird, paranoid, and bossy, says early bitcoin developer who exchanged hundreds of emails with the mysterious crypto creator." *Business Insider*, May 30, 2018. https://www.businessinsider.com/satoshi-nakamoto-was-weird-and-bossy-says-bitcoin-developer-2018-5

Bitcoin. 2018. "Frequently asked questions." https://bitcoin.org/en/faq#general

Chen, Adrian. 2016. "We need to know who Satoshi Nakamoto is." *The New Yorker*, May 9, 2016. https://www.newyorker.com/business/currency/we-need-to-know-who-satoshi-nakamoto-is

Goodman, Leah McGrath. 2014. "The face behind Bitcoin." *Newsweek*, March 6, 2014. https://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html

Greenberg, Andy. 2014. "Nakamoto's neighbor: My hunt for Bitcoin's creator led to a paralyzed crypto genius." *Forbes*, March 25, 2014. https://www.forbes.com/sites/andygreenberg/2014/03/25/satoshi-nakamotos-neighbor-the-bitcoin-ghostwriter-who-wasnt/#a796b214a37d

L. S. 2015. "Who is Satoshi Nakamoto?" *The Economist*, November 2, 2015.www.economist.com/the-economist-explains/2015/11/02/who-is-satoshi-nakamoto

Nakamoto, Satoshi. 2008. "Bitcoin: A peer-to-peer electronic cash system." https://bitcoin.org/bitcoin.pdf

Pearson, Jordan. 2017. "Former Bitcoin developer shares early Satoshi Nakamoto emails." *Motherboard*, August 11, 2017. https://motherboard.vice.com/en_us/article/7xx9gb/former-bitcoin-developer-shares-early-satoshi-nakamoto-emails

Schroeder, Stan. 2017. "Bitcoin's secretive creator could become the world's first trillionaire." *Mashable*, December 12, 2017. https://mashable.com/2017/12/12/bitcoin-satoshi-trillionaire/#R3yB8YJpqZqm

Wallace, Benjamin. 2011. "The rise and fall of Bitcoin." *Wired*, November 23, 2011. https://www.wired.com/2011/11/mf-bitcoin/

NATIONAL CYBER INVESTIGATIVE JOINT TASK FORCE

The National Cyber Investigative Joint Task Force (NCIJTF) is a federal, multiagency task force in the United States. It was founded in 2008 to better respond to increasing cybercrime threats. To do this, NCIJTF helps coordinate cybercrime response efforts and helps facilitate the sharing of information with member agencies regarding cybercrime threats (Federal Bureau of Investigation, 2019). The task force is composed of over 20 government agencies, with the FBI being the lead agency. The other agencies include the National Security Agency (NSA), the Secret Service, the Department of Defense (DoD), and various units of the U.S. military (Office of the Inspector General, 2011). NCIJTF also coordinates cybercrime response efforts with international governmental agencies and companies in the private sector (Finklea, 2017).

In the United States, there are three areas the government focuses on with any cyberattack: threat response, asset response, and intelligence support. The purpose of NCIJTF is to respond to cyber threat. This primarily includes the investigation of a cyberattack, determining who committed the attack, and making the appropriate arrests. The DHS focuses on assets—helping those affected by a cyberattack protect impacted assets (e.g., computers, data bases) and mitigate the harm from such an attack. The Office of the Director of National Intelligence focuses on intelligence support—assessing and sharing threat awareness (Finklea, 2017).

One of the initiatives of NCIJTF has been Operation Clean Slate. The focus of the operation has been to eradicate botnets affecting the United States. This operation was responsible for disrupting the GameOver Zeus botnet, which led to the indictment of its administrator, Evgeniy Mikhailovich Bogachev of Russia (Department of Justice, 2014; Finklea, 2017).

There have been criticisms of the NCIJTF. In 2011, an investigation by the Office of the Inspector General found that the NCIJTF was not—as it was designed to do—sharing pertinent cybercrime information with all of its member agencies. That same investigation found that the NCIJTF had not been established in all of the FBI's field offices. Also, it appears that a perception existed that the NCIJTF was not as much a multiagency task force as it was an extension of the cyber division of the FBI (Finklea, 2017). A subsequent investigation by the Office of the Inspector General in 2015 found that these issues had been improved upon. However, there were other issues noted in the report. NCIJTF had difficulty recruiting and retaining personnel, and it faced challenges sharing information with private-sector entities.

See also: Bots and Botnets; Federal Bureau of Investigation; GameOver Zeus Botnet; Secret Service

Further Reading

Department of Justice. 2014. "U.S. leads multi-national action against GameOver Zeus botnet and Cryptolocker ransomware, charges botnet administrator." Federal Bureau of Investigation, June 2, 2014. https://www.fbi.gov/news/pressrel/press-releases/u.s.-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware-charges-botnet-administrator

Federal Bureau of Investigation. 2019. "National cyber investigative joint task force." https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force

Finklea, Kristin. 2017. "Justice Department's role in cyber incident response." Congressional Research Service, August 23, 2017. https://fas.org/sgp/crs/misc/R44926.pdf

Office of the Inspector General. 2011. "The Federal Bureau of Investigation's ability to address the national security cyber intrusion threat." Department of Justice. https://www.hsdl.org/?abstract&did=6578

Office of the Inspector General. 2015. "Audit of the Federal Bureau of Investigation's implementation of its next generation cyber initiative." Department of Justice. https://oig.justice.gov/reports/2015/a1529.pdf

NATIONAL CYBERSECURITY ALLIANCE

The National Cybersecurity Alliance (NCSA) is an organization that seeks to improve education and knowledge about computer safety as a way to help individuals and companies keep their personal and business data protected from acts of cybercrime. This is done through the creation of partnerships between public and private organizations that set forth various programs geared toward protecting computer systems. The group recognizes that strong cybersecurity policies must exist in order for there to be accessible information as well as dependable and safe commerce on the internet. The NCSA believes that safe and secure online activity must be a shared responsibility and it works toward that goal. While the internet can provide tremendous benefits, it can also be a very dangerous place, but people and companies can limit that risk if they take precautions. It must be a shared task between all citizens to be effective.

One way the NCSA does this is through a program called "Stop. Think. Connect." This program is an online education and awareness effort. Created in 2009, the program was the product of input from officials in private companies, nonprofit organizations, and government leaders. The program provides resources (posters, videos, and statistics) free to any interested individual that they can use to help others know more. They stress the need to secure networks in businesses but also in the home, and not to forget the security of mobile devices. They also help people know what to do if they are the victim of a cyberattack.

Members of the organization also work to increase the number of degree programs in cybersecurity at colleges and universities. These programs are increasing in frequency as there is a greater need for experts in cybersecurity. However, many people are still finding that they must teach themselves the skills needed to succeed in cybersecurity-related jobs.

The NCSA hopes to decrease the number of individuals teaching themselves cybersecurity skills by holding the National Cyber Security Awareness Month each year in October. Throughout the month, NCSA supports different activities that teach people how to stay safe while they use the internet. Started in 2002, and with the help of the U.S. Department of Homeland Security, NCSA emphasizes different topics throughout the month. Some of those include cybersecurity in the workplace (which focuses on educating and training employees about safety), the future of cybersecurity and the internet (emphasizing trends and new technologies), careers in cybersecurity, and techniques to protect critical infrastructure (i.e., transportation, power grids, financial institutions) from cyberthreats.

NCSA also holds Data Privacy Day each year on January 28 as a way to give tribute to Convention 108, the international treaty on privacy and data protection. This is a day when the importance of protecting an individual's private data is the focus of activities on an international scale. Throughout the day, the NCSA holds sessions to inform the public about how their personal information can be accessed and shared with other organizations, often without permission or the knowledge of the individual. The activities not only focus on ways that individuals can protect their information but also give attention to ways businesses can protect the privacy of customer or client data. The sessions are live-streamed so people around the globe can attend. In 2019, participants included representatives from the Federal Trade Commission, Verizon, Visa, the Identity Theft Resource Center, Women in Security and Privacy, ConnectSafely.org, Microsoft, The Identity Theft Resource Center, and LinkedIn.

In their newsletter, NCSA offers tips to keeping a family's data protected and safe. Many families keep personal information such as health or financial records stored on their personal computers, yet do not take actions to protect that data. Children (and adults) may unknowingly "overshare" information on social media platforms. NCSA provide hints and tips for preventing such oversharing, and how to help children understand how to prevent sharing too much information online. They also provide tops for keeping income information secure year-round, but particularly through tax season.

For those who want to get involved, the NCSA has a Champion program. These are organizations such as schools, nonprofit groups, government agencies, or individuals who want to work toward a more secure internet. NCSA provides many opportunities for those who want to help others know more about cybersecurity. People and groups can also get involved on social media.

See also: Cybersecurity; Identity Theft; Prevention; Vulnerability

Further Reading

Ensign, Rachel Louise. 2013. "More colleges offer programs in cybersecurity." *The Wall Street Journal*, October 8, 2013. https://www.wsj.com/articles/more-colleges-offer-programs-in-cybersecurity-1380814820

Krebs, Brian. 2004. "Tougher cyber-security measures urged." *Washington Post*, December 8, 2004. http://www.washingtonpost.com/wp-dyn/articles/A45622-2004Dec7.html

Mele, Christopher, and Victor Daniel. 2017. "10 concerts, one's a lie? Be cautious, experts say." *New York Times*, April 28, 2017. https://www.nytimes.com/2017/04/28/technology/facebook-concerts-attend.html

National Cybersecurity Alliance. 2019. https://staysafeonline.org/about-us/

Singletary, Michelle. 2017. "Protect your social security benefits after data breaches: Identity thieves could apply for retirement or disability money in your name." *Washington Post*, October 6, 2017. https://www.washingtonpost.com/business/get-there/protect-your-social-security-benefits-after-data-breaches/2017/10/06/54a14d5a-a6f0-11e7-b3aa-c0e2e1d41e38_story.html

NATIONAL CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION ACT OF 2013

U.S. Representative Michael McCaul (R-TX) proposed the National Cybersecurity and Critical Infrastructure Protection Act of 2013 on December 11, 2013. The act would give the secretary of Homeland Security the ability to conduct cybersecurity strategies that would help the United States defend, mitigate, respond to, or recover from cyberattacks made against the country's critical infrastructures. This includes facilities such as chemical plants, dams, nuclear reactors, financial institutions, and transportation systems. The House passed the bill in a voice vote on July 28, 2014. However, the bill was referred to the Senate Committee on Homeland Security and Government Affairs, where it remains.

According to the legislation, a cyber incident is defined as: an incident, or an attempt to cause an incident, that if successful, would (1) jeopardize the security, integrity, confidentiality, or availability of an information system or network or any information stored on, processed on, or transiting such a system; (2) violate laws or procedures relating to system security; acceptable use policies, or acts of terrorism against such a system or network; or (3) deny access to or degrade, disrupt, or destroy such a system or network or defeat an operations or technical control of such a system or network.

The bill included provisions for the Secretary of Homeland Security to coordinate the activities of all federal, state, and local governments, laboratories, critical infrastructure owners and operators, and other entities to accomplish the following goals:

1. Facilitate a national effort to strengthen and maintain the nation's critical infrastructure from cyber threats;
2. Ensure that the policies and procedures of the DHS assist the owners and operators of critical infrastructure in receiving appropriate and timely cyber threat information when needed;
3. Seek expertise in industry sector-specific areas in order to develop voluntary security and resiliency strategies and to ensure that the allocation of federal resources is cost effective and reduces the burdens on the owners and operators of critical infrastructure;
4. Provide risk management assistance to groups when requested, as well as provide educational services to owners and operators of critical infrastructure facilities; and
5. Coordinate a strategy for research and development for developing technologies pertaining to cyber security.

A key provision of the proposal included the goal of establishing a National Cybersecurity and Communications Integration Center (NCCIC) that would share information about cyber threats and attacks with the owners and operators of critical infrastructure, as well as with government agencies. Agencies would be required to provide NCCIC with any information on cyber incidents (data breaches) or threats, which would then be shared as needed with others. The members of the NCCIC would include one ISAC (or Information Sharing and Analysis Center), the Multi-State Information Sharing and Analysis Center, the U.S. Computer Emergency Readiness Team, the Industrial Control System Cyber Emergency Response Team, and the National Coordinating Center for Telecommunications.

See also: CAN-SPAM Act of 2003; Computer Fraud and Abuse Act of 1986; Cybersecurity Act of 2012; Cybersecurity Enhancement Act of 2014; Cybersecurity Workforce Assessment Act of 2015

Further Reading

H.R. 3696. https://www.gpo.gov/fdsys/pkg/BILLS-113hr3696eh/pdf/BILLS-113hr3696eh.pdf

H.R.3696—National Cybersecurity and Critical Infrastructure Protection Act of 2014. Congress.gov. https://www.congress.gov/bill/113th-congress/house-bill/3696

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY FRAMEWORK

The Cybersecurity Framework, developed by the National Institute of Standards and Technology (NIST), outlines a plan to increase the nation's cybersecurity while at the same time protect personal privacy of users. The plan was initiated in 2014 in response to President Barack Obama's Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." In this document, President Obama stated that the nation must work to increase the security and resiliency of the nation's critical infrastructure and related cybersecurity framework. He described the interconnectivity of the nation's infrastructure (i.e., the elements that are needed for the country operate such as agriculture, communications, manufacturing, energy and banking) with the cyberenvironment. Each of these elements rely on computers and the internet to function, and a successful cyberattack on one of them could not only bring down that sector but affect others as well. Because of the risk of great harm that could result from a cyberattack, Obama sought to provide measures to improve the security of the country's cyber system. Congress assisted this initiative when it passed the Cybersecurity Enhancement Act of 2014 (Public Law 113-274).

Obama asked that NIST, part of the U.S. Department of Commerce, establish a framework that would promote "efficiency, innovation and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties" (Obama, 2013). NIST created a document with the cooperation from both the private sector and government officials. It is a way for organizations and businesses to become more aware of cyberthreats and to help them plan for an attack if it were to happen. It is also a way to help an organization set priorities for where to invest money so they can manage cybersecurity risks in a way that is cost-effective but without adding additional regulations. The document, "Framework for Improving Critical Infrastructure Cybersecurity," was issued in February 2014.

The framework was comprised of three sections: the Framework Core, the Framework Profile, and the Framework Implementation tiers. The Framework Core includes activities that are common to all infrastructure that allow for communication between them, is based on industry standards and practices, and includes five functions: identify, protect, detect, respond, and recover. The Framework Profile includes individual, unique organizational approaches to enhance cybersecurity and includes both a "current" profile that outlines current objectives and a "target" profile with ways to improve an agency's cybersecurity. The Framework Implementation tiers identify the degree to which an organization contains the elements defined in the Framework; they can range from partial to adaptive (partial, risk informed, repeatable, adaptive).

The framework also includes measures that are geared to protect the privacy of individual users. A person's information may be at risk. Information is gathered, maintained, or even disclosed by organizations. At times, there may be overcollection or over-retention of personal information, and this information may be accidentally disclosed. Organizations have a responsibility to protect all information they gather on an individual, and to ensure that a person's personal information remains safe.

The framework is voluntary and applies to all organizations regardless of their size, complexity, or purpose. The intent of the report is not to replace an organization's existing cybersecurity plan, but rather to enhance it or even rearrange a plan to make it more efficient. The general concepts in the plan should be modified, if needed, to fit the individual agency's needs, threats and vulnerabilities. The goal is to increase the security of the nation's cybersecurity and enable organizations to be resilient to possible attacks and recover quickly from them. NIST points out that the framework is not just intended for use by organizations in the United States; it can be used by organizations around the world, which would also permit greater communication and an even more secure cyber system. The department and stakeholders continue to review the report and update it as needed to keep it current.

See also: Cybersecurity; Data Sovereignty; President and Cybercrime

Further Reading

National Institute of Standards and Technology. 2014. "Framework for Improving Critical Infrastructure Cybersecurity." February 12, 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Obama, Barack. 2013. "Executive Order 13636: Improving critical infrastructure cybersecurity." Federal Register 78, 33: 11739–11744. https://www.govinfo.gov/content/pkg/FR-2013-02-19/pdf/2013-03915.pdf

Shackelford, Scott J., Andrew A. Proia, Brenton Marell, and Amanda N. Craig. 2015. "Toward a global cybersecurity standard of care?: Exploring the implications of the 2014 NIST Cybersecurity Framework on shaping reasonable national and international cybersecurity practices." *Texas International Law Journal* 50, 2: 303–353.

Stone, Jeff. 2018. "Amid national security warnings, NIST adds supply-chain security to cyber framework." *Wall Street Journal*, April 19, 2018. https://www.wsj.com/articles/amid-national-security-warnings-nist-adds-supply-chain-security-to-cyber-framework-1524175900

NEWS CORP HACKING

News Corp is a large corporation that oversees several different businesses. This includes several news organizations. From 2000 to 2006, some of the British news organizations overseen by News Corp—*News of the World* and *The Sun*, specifically—were involved in phone hacking (Childress and Gavett, 2012). Those whose phones were hacked include celebrities, politicians, soldiers, and crime victims.

The hacking conducted by News Corp consisted of employees or contractors accessing the voice mails of people targeted for media coverage by the news outlets overseen by News Corp. This was done to give journalists an edge in their reporting, possibly uncovering new stories or new angles to stories by virtue of the hacked information (BBC, 2014). Evidence of possible phone hacking first emerged in 2005. In November of that year, News of the World published a story about a knee injury sustained by Prince William. The information in the article was not public knowledge, and officials for the royal family insist the information could only have come from Prince William's private voice mails (BBC, 2014; CNN, 2019). In 2007, two people—private investigator Glenn Mulcaire and News of the World editor Clive Goodman—pleaded guilty to hacking those voice mails. Goodman was sentenced to four months in jail, and Mulcaire—who had pleaded guilty to additional hacking charges related to the voice mail of other victims—was sentenced to six months (Tryhorn, 2007). Andy Coulson—also an editor at News of the World—resigned in 2007 following the convictions of Mulcaire and Goodman, though he denied knowing about the phone hacking that had taken place while there (CNN, 2019).

This was not the end of this scandal, however. A sizeable amount of evidence was seized from Mulcaire when he was initially arrested. It was found that Mulcaire had hacked thousands of phones for News of the World. Further investigation of that and other evidence ultimately led to additional criminal charges. (BBC, 2014). There was evidence to suggest that News Corp had attempted to cover up their phone-hacking endeavors. News of the World had reached several confidential settlements with those whose phones it had hacked. This kept the scope of its phone hacking efforts hidden for a time (BBC, 2014). After an investigation by law enforcement was initiated against News of the World for phone hacking, it engaged in further phone hacking of the investigators from Scotland Yard who were investigating it (Boyle, 2015).

The phone hacking engaged in by News of the World extended beyond public figures. It was found that it had hacked the phones of soldiers who died in the wars in Iraq and Afghanistan (Boyle, 2015). It was also reported that News of the World had attempted to hack into the phones of victims of the September 11 terrorist attack in New York (Daily Mail Reporter, 2011), though an investigation by the FBI determined there was insufficient evidence to find this actually happened (Flock, 2011). Perhaps the most egregious evidence against News of the World was evidence of its hacking of the phone of Milly Dowler—a British teenager who was kidnapped in 2002 and was ultimately murdered. Before it had been discovered that Dowler had been murdered, News of the World hacked into her voice mail. Reporters deleted voice mails in her mailbox to free up space for new messages to be left. Dowler's parents, seeing activity on their daughter's voice mailbox, believed it was evidence that their daughter may still be alive and was listening to her voice mail (Boyle, 2015). News of this was made public on July 4, 2011. News of the World shut down permanently six days later (CNN, 2019).

Several other people faced criminal charges arising from this phone hacking. Many of these people pleaded guilty to their involvement in 2014 and 2015. Mulcaire—the investigator previously convicted for other charges stemming from the phone-hacking scandal—was one of these people. He was given a six-month suspended jail term. Three editors pleaded guilty: James Weatherup, Greg Miskiw, and Ian Edmondson. Weatherup received a four-month suspended jail sentence, Miskiw received a six-month jail sentence, and Edmondson received an eight-month jail sentence (Halliday, 2014; Telegraph, 2014). Three reporters pleaded guilty as well: Neville Thrulbeck, Dan Evans, and Jules Stenson. Thurlbeck received a six-month jail sentence, Evans received a 10-month suspended jail sentence, and Stenson received a four-month suspended jail sentence (O'Carroll, 2015; Telegraph, 2014). Others who were charged opted to go to trial. Many that went to trial were acquitted of the charges against them. Those acquitted were editors Rebekah Brooks, Stuart Kuttner, and Neil Wallis (BBC, 2014; O'Carroll, 2015). Coulson—the editor who resigned from News of the World in 2007 following the initial round of criminal charges against Mulcaire and Goodman—was found guilty at trial for his involvement in the phone hacking scandal. He was sentenced to eighteen months in jail (Cowell and Bennhold, 2014).

Criminal charges were filed against individuals for crimes other than phone hacking as well. In 2011, allegations arose that the London Metropolitan Police were involved in the phone hacking scandal. Amid these allegations, both the commissioner and assistant commissioner of the London Metropolitan Police—Paul Stephenson and John Yates respectively—resigned (CNN, 2019). Neither has faced criminal charges. However, two employees of News of the World—Coulson and Goodman—were charged with conspiracy to illegally pay officers for directory information. The jury was hung as to a verdict in that case (BBC, 2014). The two face the possibility of a retrial on those charges (Cowell and Bennhold, 2014). Criminal charges were also filed against Charlie Brooks (husband of editor Rebekah Brooks), Cheryl Carter (Rebekah Brooks's personal assistant), and Mark Hanna (head of security) for conspiracy to conceal information from the police in the course of their investigation into the phone hacking matter. All three were acquitted of those charges at trial (BBC, 2014).

There have been other repercussions for News Corp beyond the criminal charges against many of its reporters and editors. It has paid out significant amounts of money in settlement with the victims of the phone hacking. The family of Dowler received over $3 million. Several others received funds, the amounts of which were not disclosed. News of the World established a compensation program in 2011 to provide compensation to victims (CNN, 2019). In 2012, Rupert Murdoch, founder of News Corp, resigned from his board positions at the British newspapers he oversaw and relinquished his title executive chairman for News Corp's publishing unit in the United Kingdom (CNN, 2019; Childress and Gavett, 2012).

See also: Federal Bureau of Investigation; Hacker and Hacking

Further Reading

BBC. 2014. "Phone-hacking trial explained." June 25, 2014. https://www.bbc.com/news/uk-24894403

Boyle, Christina. 2015. "British phone-hacking scandal was a low point for Rupert Murdoch." *Los Angeles Times*, June 11, 2015. https://www.latimes.com/world/europe/la-fg-british-scandal-murdoch-20150611-story.html

Childress, Sarah, and Gretchen Gavett. 2012. "The News Corp. phone-hacking scandal: A cheat sheet." PBS, July 24, 2012. https://www.pbs.org/wgbh/frontline/article/the-news-corp-phone-hacking-scandal-a-cheat-sheet/

CNN. 2019. "UK phone hacking scandal fast facts." April 29, 2019. https://www.cnn.com/2013/10/24/world/europe/uk-phone-hacking-scandal-fast-facts/index.html

Cowell, Alan, and Katrin Bennhold. 2014. "Andy Coulson gets 18 months in tabloid phone hacking." *New York Times*, July 4, 2014. https://www.nytimes.com/2014/07/05/world/europe/andy-coulson-to-be-sentenced-in-phone-hacking-case.html

Daily Mail Reporter. 2011. "News of the World is accused of hacking phones of 9/11 victims." July 14, 2011. https://www.dailymail.co.uk/news/article-2013334/News-World-hacked-phones-September-11-victims-claims-ex-cop.html

Flock, Elizabeth. 2011. "Did News of the World hack 9/11 victims phones? 'No hard evidence,' says FBI." *Washington Post*, August 15, 2011. https://www.washingtonpost.com/blogs/blogpost/post/did-news-of-the-world-hack-911-victims-phones-no-hard-evidence-says-fbi/2011/08/15/gIQATqTsGJ_blog.html?utm_term=.1a5b49945ca6

Halliday, Josh. 2014. "Ian Edmondson jailed for eight months over phone hacking." *The Guardian*, November 7, 2014. https://www.theguardian.com/media/2014/nov/07/ian-edmondson-jailed-eight-months-phone-hacking-news-of-the-world

O'Carroll, Lisa. 2015. "Ex-News of the World features editor gets four-month suspended sentence." *The Guardian*, July 6, 2015. https://www.theguardian.com/uk-news/2015/jul/06/ex-news-of-the-world-features-editor-jules-stenson

Telegraph. 2014. "Jules Stenson admits phone hacking at News of the World." December 12, 2014. https://www.telegraph.co.uk/news/uknews/phone-hacking/11290234/Jules-Stenson-admits-phone-hacking.html

Tryhorn, Chris. 2007. "Clive Goodman sentenced to four months." *The Guardian*, January 26, 2007. https://www.theguardian.com/media/2007/jan/26/newsoftheworld.pressandpublishing1

NIMDA

In September 2001, a new computer worm and virus, called Nimda, or "admin" backward, appeared on the internet and spread quickly around the globe. The malware affected those who were running Microsoft Windows 95, 98, 2000, or XP and became one of the most destructive worms launched. It also was referred to as Concept5, Code Rainbow, and Minda. The virus proved to be costly for private businesses and resulted in billions of dollars in damages.

The source of the virus is unknown. A preliminary report alleged that the Nimda worm originated in China. Others were fearful that it could be associated with the September 11, 2001, terrorist attacks that happened just prior to the worm being released. Further investigation found no evidence of a link between the attacks and the malware. However, experts indicated that there was an increase in the number of people and businesses using e-mail in the weeks after the terrorist attacks, which only served to spread the virus.

The worm spread between computers in a variety of ways, which in part accounted for the immediate spread of the malware. The worm was delivered to users through an e-mail attachment with the subject line that said "Read Me." When a user opened the attachment, the worm was immediately uploaded without the user's knowledge. The malware then scanned the user's contacts and sent infected e-mails to those addresses. The virus also spread from compromised websites. If a user visited a website that had been infected, the virus would download onto the system and then search for additional contacts in a similar fashion. The third way the virus spread was through vulnerabilities or backdoors in computer networks that had been left open by other worms and viruses. This way, the worm could travel from one computer system or network to another system or network.

Once a computer was infected with Nimda, it infected files that were on the computer, so opening the program caused the worm to run first. The virus gave the attacker full administrative authority over the infected computer and provided them with the ability to access files on the computer and steal information from the user. The virus did not harm computer hardware or destroy any data on the infected computer. Nimda also clogged the internet because it created a massive amount of internet traffic, and it shut down websites that were infected. This affected both the owner of the website and the potential visitor to the site.

Not only did Nimda scan for contacts upon being uploaded, but 10 days after the initial infection, it scanned for contacts again. New forms of the Nimda worm were discovered in October and then in November 2001, again spreading the malware to millions of users.

The Nimda worm made multiple modifications to an infected computer system. It also wrote a copy of itself to each directory. This made it difficult to delete. In order to fully remove the virus from a computer, a user was forced to reformat any drives that had become infected and then reinstall the system software. It was necessary for any patches to be applied to alleviate any backdoors or vulnerabilities that may have allowed the virus to attack the computer in the first place.

In order to keep computers free from viruses, it is essential that users install antivirus software and keep it updates. It is also essential that they apply patches if they are available and be cautious when sharing files from others.

See also: Code Red; Malware; Worm

Further Reading

Balthrop, Justin, Stephanie Forrest, M. E. J. Newman, and Matthew M. Williamson. 2004. "Technological networks and the spread of computer viruses." *Science* 304 (April 23): 5670, 527–529.

CBS News. 2001. "A worm named Nimda." September 8, 2001. https://www.cbsnews.com/news/a-worm-named-nimda/

SANS Institute InfoSec Reading Room. "Nimda worm—Why is it different?" https://www.sans.org/reading-room/whitepapers/malicious/nimda-worm-different-98

Shiver, Jube. 2001. "New internet worm hits computers." *Los Angeles Times*, September 19, 2001.

Thomas, Timothy L. 2003. "Al Qaeda and the internet: The danger of 'cyberplanning.'" Defense Technical Information Center, Foreign Military Studies Office (Army), Fort Leavenworth, KS. http://www.dtic.mil/dtic/tr/fulltext/u2/a485810.pdf

NORTH KOREA

Gauging the amount of cybercrime that occurs in North Korea is difficult as it does not appear that the country releases statistics regarding its criminal justice system. The likelihood of cybercrime victimization would seem to be low, as citizen access to the internet is severely restricted. Access by North Korean citizens to the

World Wide Web is limited to elite members of society—roughly a few thousand citizens in total (Williams, 2010). North Korea does have local internet available to citizens—known as the *kwangmyong*—that only permits users to view North Korea–based websites (Amnesty International, 2019). Even though the kwangmyong is available for citizens to use, the cost of obtaining access is prohibitive for many citizens. Permission to access the kwangmyong must be obtained from the North Korean government, and that permission can cost up to three times the average monthly salary in North Korea (Wright and Urban, 2017).

North Korea's internet scheme is designed to censor information unfavorable to the North Korean government from entering the country. Accordingly, those who access unauthorized information are deemed to have committed a crime. It is not just through the internet that such information could be obtained, however. The North Korean government is concerned that such information could be obtained phone calls with people outside of North Korea. Thus, possession of a cellular phone that is able to make a call outside the country is likewise considered a crime. The punishment for committing one of these crimes can be severe. Possible sentences include being sent to a labor camp or even being executed (Amnesty International, 2019; Wright and Urban, 2017).

Whereas the domestic internet situation in North Korea is relatively unsophisticated, its cyberattack capabilities appear more evolved. North Korea's cyberattack operations appear to be housed in its Reconnaissance General Bureau (RGB) and coordinate attacks with the Korean People's Army (KPA). The number of hackers working for North Korea is estimated to be between 3,000 and 6,000. Many of these hackers live outside of North Korea where they can utilize the advanced technological infrastructure in other countries (Chanlett-Avery et al., 2017). North Korea has carried out cyberattacks on entities from several foreign countries, including the United States, Israel, South Korea, Russia, Chile, and Turkey (Center for Strategic and International Studies, 2019). North Korea's motivations for carrying out cyberattacks appear to be similar to those of other countries, such as espionage and disrupting the operations of countries viewed as hostile to North Korea. One of North Korea's motivations that it does not necessarily share with other countries is financial gain (Campbell, 2017). North Korea has carried out cyberattacks on several economic institutions. As of 2018, North Korea cyberattacks attempted to steal a combined amount of over $1 billion and successfully stole over $100 million (Cohen and Marquardt, 2018). The reason North Korea engages in theft-based cybercrimes appears to be circumvent sanctions imposed on it by other countries. Those sanctions have had an economic impact on North Korea, and cybercrime has provided an avenue for the country to generate income (So-hyun, 2019). One attack carried out by North Korea for financial gain was the release of WannaCry malware. WannaCry, released in 2017, was ransomware that affected approximately 300,000 people worldwide. It was able to obtain $140,000 through use of the ransomware. North Korea has also used direct cyberattacks for financial gain. In 2016, it was able to infiltrate the networks of banks in Bangladesh and Southeast Asia and transfer money out of those banks to itself. The thefts totaled roughly $81 million (Chanlett-Avery et al., 2017).

Another mechanism that North Korea uses to circumvent sanctions is cryptocurrencies. Where cryptocurrencies are more difficult to trace than standard currency, North Korea can more easily obfuscate the origins of its illegal gains though cryptocurrency. This does not mean it is completely untraceable, however. It appears that the funds obtained through the use of the WannaCry ransomware were attained as bitcoin. North Korea has not converted the bitcoin to standard currency as law enforcement was able to track down the Bitcoin as the proceeds of the ransomware (Chanlett-Avery et al., 2017). North Korea is not obtaining bitcoin exclusively through illegal means. It mines bitcoin as well (Pham, 2017). Legally obtained cryptocurrencies also permit North Korea to circumvent sanctions as the added anonymity of cryptocurrencies can help shield economic transactions between North Korea and entities based in countries that have sanctioned North Korea. North Korea is not the only country that uses cryptocurrency to circumvent sanctions; it appears Russia and Iran may do so as well (Fruth, 2018).

Perhaps the best-known cyberattack perpetrated by North Korea was its hack of Sony Pictures in 2014. The hack resulting in the destruction of data on Sony's network and the theft of information that was later released to the public. The hack appears to be retaliatory. Sony was in the process of releasing *The Interview*—a movie whose plot involved the assassination of North Korean president Kim Jong-un. North Korea denied its involvement in this attack, though it applauded the hackers that had perpetrated the cyberattack (Chanlett-Avery et al., 2017). One North Korean citizen—Park Jin Hyok—was criminally charged in the United States for his involvement in the hack of Sony, as well as for his involvement in the WannaCry ransomware attack and the hack of banks in Bangladesh. The criminal complaint against Hyok was unsealed in 2018. In the complaint, Hyok is alleged to be a member of a North Korean–sponsored hacking team known as the Lazarus Group (United States Department of Justice, 2018).

North Korea has been the victim of state sponsored attacks as well, particularly from the United States. In 2017, there was indication that the U.S. Cyber Command conducted a DDoS attack on North Korea's RGB. In 2013, North Korea blamed the United States and South Korea for a similar attack that restricted internet access in the country (Center for Strategic and International Studies, 2019).

See also: Bitcoin; Cryptocurrency; Cyberwarfare; Hacker and Hacking; International Issues; Political Uses; Ransomware; Sony Pictures Entertainment Hack

Further Reading

Amnesty International. 2019. "North Korea: Connection denied." https://www.amnesty.org/en/latest/campaigns/2016/03/north-korea-connection-denied/

Campbell, Charlie. 2017. "The world can expect more cybercrime from North Korea now that China has banned its coal." *Time*, February 20, 2017. http://time.com/4676204/north-korea-cyber-crime-hacking-china-coal/

Center for Strategic and International Studies. 2019. "Significant cyber incidents." Center for Strategic and International Studies. https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

Chanlett-Avery, Emma, Liana W. Rosen, John W. Rollins, and Catherine A. Theohary. 2017. "North Korean cyber capabilities: In brief." Congressional Research Service, August 3, 2017. https://fas.org/sgp/crs/row/R44912.pdf

Cohen, Zachary and Alex Marquardt. 2018. "North Korean hackers tried to steal over $1 billion, report says." CNN, October 3, 2018. https://www.cnn.com/2018/10/03/politics/north-korea-hackers-cybercrimes/index.html

Fruth, Joshua. 2018. "'Crypto-cleansing': Strategies to fight digital currency money laundering and sanctions evasion." *Reuters*, February 13, 2018. https://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-cleansing-strategies-to-fight-digital-currency-money-laundering-and-sanctions-evasion-idUSKCN1FX29I

Pham, Sherisse. 2017. "North Korea may be making a fortune from bitcoin mania." CNN, December 13, 2017. https://money.cnn.com/2017/12/12/technology/north-korea-bitcoin-hoard/index.html

So-hyun, Kim. 2019. "Sanctions motivated NK cybercrimes: US officials." *The Korea Herald*, May 30, 2019. http://www.koreaherald.com/view.php?ud=20190530000496

United States Department of Justice. 2018. "North Korean regime-backed programmer charged with conspiracy to conduct multiple cyber attacks and intrusions." September 6, 2018. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

United States Department of State. 2012. "Country reports on human rights practices for 2012: Korea, Democratic People's Republic of." https://2009-2017.state.gov/j/drl/rls/hrrpt/2012humanrightsreport/index.htm?year=2012&dlid=204210#wrapper

Williams, Martyn. 2010. "North Korea moves quietly onto the internet." *Computerworld*, June 10, 2010. https://www.computerworld.com/article/2518914/north-korea-moves-quietly-onto-the-internet.html

Wright, Mike, and David Urban. 2017. "Brutal and inhumane laws North Koreans are forced to live under." *The Telegraph*, September 19, 2017. https://www.telegraph.co.uk/news/2017/09/19/brutal-inhumane-laws-north-koreans-forced-live/

O

OPEN-SOURCE

”Open-source” is a term used for programming code that is open and available for anyone to use and modify. Depending on how the developer decides to treat their open-source code, it could be in the public domain or it could have a license that allows anyone to use it for whatever purpose they want. The practical difference between the two is that a developer who licenses the code could put some restrictions on how the code can be used (e.g., a developer could restrict the ability of a user to copy and sell the open-source code) and can possibly rescind that license at a later date. Various open-source licenses are provided by the Open Source Initiative (Open Source Initiative, 2018), though a developer is not obligated to use one of these licenses for an open-source project. Failure to abide by the terms of a license would be a violation of the developer's intellectual property rights.

Open-source projects are supported by several large technology corporations, including Adobe, Facebook, Google, and Microsoft. There are advantages for these and other companies to do so. The quality of the software produced through the use of open-source code can often be better because of the number of people who are then able to work on the software. Open-source software is also more customizable for users, and the support for users can be more expansive as a result of user communities that often arise (Noyes, 2010).

Freeware is similar to open-source code, but there is a legal difference. Freeware is a complete piece of software that is released by its developer free of charge to the public. Thus, just like open-source code, users can download and use freeware without violating the developer's intellectual property rights. However, with freeware, users are not permitted to modify the code of that software and redistribute it—something that generally would be permitted with open source code (Rey, 2009). Attempts to adjust the code of freeware and redistribute the software to others would violate the property rights of the developer.

Shareware is also similar to open-source code, as well as freeware. Shareware is software that is offered to the public free of charge on a trial basis but later requires payment if a user wishes to keep the software (Rey, 2009). It differs from open-source code the same way freeware differs from open-source code—users of the software are not permitted to alter the code of the software and redistribute it. It differs from freeware in the length of time that users can use the software for free—freeware is free indefinitely, where shareware is only free to use for a limited time (whatever the developer specifies). If a user were to use the software without paying for it past the trial period, that would violate the developer's intellectual property rights.

These different designations of code and software illustrate how there can be different levels of "free" when it comes to software. Some developers relinquish all their intellectual property rights to a piece of software, as with source code generally. In such instances, not only is the software free of charge, it is also free of intellectual property right restrictions. Other developers may provide their software free of charge, but they will retain their intellectual property rights, as with freeware. In that instance, the software is only free in regards to the cost and your ability to possess it. It is not free of intellectual property right restrictions, as the developer retained them. Others still may allow their software to be used free for a limited period of time, as with shareware. In that instance, the software is free to use during the trial period, but it is not free to possess indefinitely, nor is it free of intellectual property right restrictions.

In addition to the general distinctions above, a developer could retain or relinquish other intellectual property right protections as part of their license for the software. As noted above, some open-source code is released under a license whereby a developer places some restrictions on the use of the code. For example, a developer could release code for general use as long as anyone who uses it gives the developer credit. Likewise, a freeware developer could permit users to modify the code for personal use (for a user to make a piece of freeware compatible with other programs, for example) but not to distribute that modified version of the software to others.

See also: Abandonware; Copyright Infringement; Public Domain

Further Reading

Noyes, Katherine. 2010. "10 reasons open source is good for business." PC World, November 5, 2010. https://www.pcworld.com/article/209891/10_reasons_open_source_is_good_for_business.html

Open Source Initiative. 2018. "Licenses & standards." Open Source Initiative. https://opensource.org/licenses

Rey, Sergio J. 2009. "Show me the code: Spatial analysis and open source." *Journal of Geographical Systems* 11, 2: 191–207.

OPERATION APOTHECARY

Operation Apothecary is an ongoing investigation handled by the National Intellectual Property Rights Coordination Center (part of U.S. Immigration and Customs Enforcement). Beginning in 2004, agents began to crack down on unauthorized or fake pharmaceutical sales. The costs of many prescription drugs have risen so dramatically that many people are trying to get them anywhere they are cheaper, and many people find sites online that offer cheap drugs. Unfortunately, many of those sites are not legitimate and sell counterfeit drugs or drugs not approved by the Food and Drug Administration (FDA). The drugs may have been manufactured in a facility that has unsafe or unsanitary conditions or in a facility that had no quality controls over the final product. In some cases, the drugs that are sold online are past the expiration date or are the incorrect dosage. If a person purchases these drugs, there could be serious repercussions to their health.

When a potential customer goes online to look for cheap pharmaceutical drugs, criminals will pose as a representative from a pharmaceutical company and will claim to be selling prescription drugs or the cheaper, generic drugs, often without even requiring a physician's prescription. If the patient decides to purchase the drug, they may not receive any product, or they may receive a drug that is not the one they wanted. Operation Apothecary investigates these violations of sales. The officers from Immigration and Customs Enforcement–Homeland Security Investigations (ICE–HIS) work alongside officers from Customs and Border Protection (CBP), the FDA, and the U.S. Postal Inspection Service (USPIS). They often search incoming mail at international mail branches, international courier hubs, and ports.

The investigations into illegal prescription drugs have grown to include 24 countries. In 2009, law enforcement from around the world, including Interpol in Europe and the Drug Enforcement Agency (DEA) in the United States, raided mail centers to look for packages containing drugs. The officers examined over 7,000 suspicious packages in their attempt to not only track down the drugs themselves but also to identify patterns of drug shipments. In all, the officers found almost 800 packaged of suspicious prescription drugs. They were also able to close 68 online pharmacies.

See also: Economy, Effects on; Federal Bureau of Investigation

Further Reading

Mui, Ylan Q. 2009. "Growth of counterfeit drugs parks international response." *Los Angeles Times*, November 21, 2009. http://articles.latimes.com/2009/nov/21/business/la-fi-counterfeit21-2009nov21

U.S. Immigration and Customs Enforcement. 2011. "Operation Apothecary." July 26, 2011. https://www.ice.gov/factsheets/ipr-apothecary

OPERATION AURORA

In 2009, the Eldergroup, based in China and having ties to the People's Liberation Army, carried out a series of sophisticated cyberattacks that exploited a zero-day vulnerability they discovered in Microsoft Internet Explorer and then relied on advanced persistent threats to target over 34 companies involved in the areas of technology, finance/banking, and defense (and others) that included Yahoo, Symantec, Morgan Stanley, Lockheed Martin, Dow Chemical and Northrop Grumman, Adobe Systems, Juniper Networks, Rackspace, and the U.S. Labor Department. The attacks were not made public until 2010 when Google chose to announce them. The attacks were nicknamed Operation Aurora by Dmitri Aplerovitch, the vice president of Threat Research at McAfee, a cybersecurity company. He based this name on the Trojan malware that the hackers used to carry out the attack, and it was the name the hackers used when referring to their plans to carry out the attacks on these companies.

The malware was spread by unwitting employees at these targeted companies who inadvertently uploaded the malware onto computers after being sent to a malicious website via e-mail or social networking. Once loaded on a computer, the malware took over the computer, allowing the offenders to steal company secrets and other information. This was the first time by a cyber-attack was used for industrial espionage by a government-sponsored hacking group. The attack was carried out smoothly and surreptitiously so that when it was first discovered, Google officials were under the assumption that it was an insider attack.

The results of Operation Aurora that were announced in 2013. According to the report, U.S. government officials reported that the hackers were able to gain access to many years' worth of sensitive data. Additionally, officials at Google reported that hackers stole some of its intellectual property and company secrets. They also claimed that the hackers stole information on human rights activists.

It was also reported by top security experts that the goal of the breach was a form of counterintelligence, specifically to discover the identities of Chinese intelligence operatives who were living in the United States and who may have been under surveillance by law enforcement in the United States. As one former official said, "Knowing that you were subjects of an investigation allows them to take steps to destroy information, get people out of the country" (Nakashima, 2013). The hackers chose companies that had been served search documents or other legal papers related to the surveillance operation or had some other information on it. For example, Google has a database with details regarding years of surveillance orders, including thousands of orders that had been issued by judges to law enforcement agents who sought permission to monitor the mail of particular suspects. That same former official indicated that Chinese hackers may have intended to deceive U.S. intelligence officials by conveying false or even misleading information.

The most sensitive documents came from the U.S. Foreign Intelligence Surveillance Court (FISA Court), which gives approval for law enforcement to carry out surveillance of foreign suspects, including spies, diplomats, or suspected terrorists. These orders, issued under the Foreign Intelligence Surveillance Act of 1978, are classified and therefore secret. Consequently, U.S. officials were concerned when informed of the breach as it may have allowed the offender to gain access to investigations that were being carried out by FBI agents on undercover Chinese agents. Officials in China denied the attacks.

In general, U.S. officials have expressed alarm when it comes to hacking by the Chinese. Intrusions have been uncovered at multiple locations, including defense contractors, aerospace companies, oil and gas companies, and even branches of the U.S. government. The FBI has investigated Chinese hacking practices and have concluded that they have stolen massive amounts of data. The director of the National Security Agency, Gen. Keith B. Alexander, has described to the theft of proprietary data as the "greatest transfer of wealth in history" (Nakashima, 2013).

In the end, Google officials chose to halt its operations in China. The company also began to notify users whose accounts may have been part of a state-sponsored attack, a practice that other e-mail providers eventually mimicked. Many governments, including France, Germany, and Australia, warned residents to consider using a browser other than Internet Explorer as a way to keep their data safe.

See also: China; Hacker and Hacking; Zero-Day Attacks

Further Reading

Nakashima, Ellen. 2013. "Chinese hackers who breached Google gained access to sensitive data, U.S. officials say." *Washington Post*, May 20, 2013. https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say

Nakashima, Ellen, and Soltani Ashkan. 2014. "FBI warns industry of Chinese cyber campaign." *Washington Post*, October 15, 2014. https://www.washingtonpost.com/world/fbi-warns-industry-of-chinese-cyber-campaign/2014/10/15/0349a00a-54b0-11e4-ba4b

Schwartz, Matthew J. 2013. "Google Aurora hack was Chinese counterespionage operation." *Dark Reading*, May 21, 2013. https://www.darkreading.com/attacks-and-breaches/google-aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060

Yadron, Danny, James T. Areddy, and Paul Mozur. 2014. "China hacking is deep and diverse, experts say." *Wall Street Journal*, May 29, 2014. https://www.wsj.com/articles/china-hacking-is-deep-and-diverse-experts-say-1401408979

Zetter, Kim. 2010. "Google hack attack was ultra sophisticated, new details show." *Security*, January 14, 2010. https://www.wired.com/2010/01/opration-aurora

OPERATION INNOCENT IMAGES

Operation Innocent Images was an investigation into online child sexual exploitation undertaken by the FBI in 1994. It was during a separate investigation into a missing child in Maryland in 1993 that this operation was founded. In that case, 10-year-old George Burdynski went missing on May 24, 1993. In the course of the investigation, it was discovered that George and his friends had visited the homes of several men in town: James Kowalski, Stephen Leak, and Joseph Lynch. Kowalski and Leak had sexually abused two of Burdynski's friends the weekend before he went missing. Kowalski invited the two boys to play video games and eat pizza. Once the boys were there, Kowalski sexually assaulted one of the boys while the other boy recorded the incident with a video camera. Leak was present and watched the incident (Johansson, 1995; McCabe, 2013). In a separate incident, Lynch sexually assaulted a friend of Burdynski's. Lynch was convicted of that crime in 1994. Kowalski and Leak were also convicted of sexual assault in 1993. In addition, Kowalski and Leak were also convicted of child pornography charges (*Washington Times*, 2002). It had been discovered that Kowalski and Leak had been using the internet not only to disseminate child pornography but also to make contact and communicate with boys and set up meetings with them (Federal Bureau of Investigation, 2018). Kowalski was at one point the prime suspect in Burdynski's disappearance, but there was not enough information to charge him with that crime (Federal Bureau of Investigation, 2018; *Washington Times*, 2002).

While the Burdynski case was never solved, the evidence of online child sexual exploitation that the FBI discovered in the course of investigating Kowalski and Leak led them to initiate Operation Innocent Images. As part of the operation, agents went online in an undercover capacity to gather information about those suspected of distributing child pornography and otherwise sexually exploiting children online. Agents posed as children, or in some cases as someone interested in obtaining child pornography, to try and lure out pedophiles (Federal Bureau of Investigation, 2018). Search warrants were executed on September 13, 1995, at over 100 locations in the United States. Computers and disks were seized as part of those search warrants. In the first few weeks following the execution of the search warrants, only 15 arrests were made. It appears as though some suspects used encryption to keep the contents of their computers inaccessible to agents when they raided those suspects' homes (Lewis, 1995).

The use of encryption by suspects to avoid law enforcement discovering digital evidence does continue to be an issue for law enforcement. In 2015, the FBI was unable to bypass the encryption on a phone belonging to suspect in a terrorism case in San Bernardino, California. The FBI sued Apple—the maker of the phone in question—to compel them to provide a bypass to encryption on its phone. Apple contested the case. The FBI was ultimately able to bypass the encryption on the phone before the issue had to be litigated (Selyukh, 2016). Cases like Operation Innocent Images and the San Bernardino case underscore law enforcement's need for encryption-breaking technology (see Fine, 2001; Lewis, 1995). It also appears that law enforcement is able to respond to that need as technology advances. Following the San Bernardino case, for example, it appears that law enforcement gained access to technology through a government contractor that likely gave them the ability to break through the encryption of any Apple phone (Brewster, 2018).

Following the completion of Operation Innocent Images in 1995, the Innocent Images National Initiative was formed that same year. The Initiative extended the investigative efforts of federal law enforcement into online child sexual exploitation. As part of the Initiative, agents employ investigative methods used in Operation Innocent Images. From its formation in 1995 through 2000, the Initiative processed over 1,000 cases that resulted in convictions (Fine, 2001). In a number of the cases that resulted in conviction during that time, it appears the sentences given to offenders were lighter than was hoped by the FBI. Judges justified those lighter sentences by noting that—among other things—FBI agents were the ones making contact with offenders, not actual children. Thus, where there was no actual harm to a child, the lighter sentence was appropriate (Will, 2000).

The FBI continues to investigate cases of child pornography and child sexual exploitation through the Innocent Images National Initiative. From its inception through 2007, the Initiative was involved in 6,800 cases that resulted in conviction (Federal Bureau of Investigation, 2018). In the fiscal year 2014–2015 alone, the Initiative was involved in 2,200 cases that resulted in conviction (United States Department of Justice, 2016). The investigation engaged in by the Initiative are done both domestically and internationally in conjunction with other investigators from other countries (Federal Bureau of Investigation, 2018).

See also: Bypass; Child Pornography; Federal Bureau of Investigation

Further Reading

Brewster, Thomas. 2018. "The Feds can now (probably) unlock every iPhone model in existence." *Forbes*, February 26, 2018. https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/#2ba8df26667a

Federal Bureau of Investigation. 2018. "Operation Innocent Images." https://www.fbi.gov/history/famous-cases/operation-innocent-images

Fine, Glenn A. 2001. *Review of child pornography and obscenity crimes*. United States Office of the Inspector General, July 19, 2001. https://oig.justice.gov/reports/plus/e0107/results.htm

Johansson, Cynthia. 1995. "Court overturns child abuse convictions." *Capital News Service*, October 25, 1995. https://cnsmaryland.org/1995/10/25/court-overturns-child-abuse-convictions/

Lewis, Peter H. 1995. "TECHNOLOGY: ON THE NET; The F.B.I. sting operation on child pornography raises questions about encryption." *New York Time*, September 25, 1995. https://www.nytimes.com/1995/09/25/business/technology-net-fbi-sting-operation-child-pornography-raises-questions-about.html

McCabe, Scott. 2013. "Cold case: Innocent Images operation began with Prince George's County case." *Washington Examiner*, April 7, 2013. https://www.washingtonexaminer.com/cold-case-innocent-images-operation-began-with-prince-georges-county-case

Selyukh, Alina. 2016. "The FBI has successfully unlocked the iPhone without Apple's help." National Public Radio, March 28, 2016. https://www.npr.org/sections/thetwo-way/2016/03/28/472192080/the-fbi-has-successfully-unlocked-the-iphone-without-apples-help

United States Department of Justice. 2016. *The national strategy for child exploitation prevention and interdiction*. https://www.justice.gov/psc/file/842411/download

The Washington Times. 2002. "Police still on 'Junior' Burdynski case." March 16, 2002. https://www.washingtontimes.com/news/2002/mar/16/20020316-041101-7781r/

Will, George F. 2000. "Nasty work." *Washington Post*, January 23, 2000. http://www.washingtonpost.com/wp-srv/WPcap/2000-01/23/090r-012300-idx.html

OPERATION MARCO POLO

Operation Marco Polo was an investigation into the dark web marketplace known as Silk Road. The operation began in 2013. Several federal agencies were involved in the operation, with the operation based out of the Homeland Security Investigations office in Baltimore, Maryland (Bearman et al., 2015a). The investigation ultimately led to Silk Road being shut down and its founder, Ross Ulbricht (also known as Dread Pirate Roberts), being arrested on October 1, 2013. Ulbricht was ultimately convicted of money laundering, computer hacking, conspiracy to traffic fraudulent identity documents, and conspiracy to traffic narcotics by means of the internet. He was sentenced to life in prison on May 29, 2015 (Segall, 2015).

Two agents—Agent Mark Force with the Drug Enforcement Administration (DEA) and Agent Jared Der-Yeghiayan with Homeland Security Investigations—were able to infiltrate Silk Road in an undercover capacity beginning in 2012. Agent Force did so by creating a fake online persona (Nob) and gaining the trust of Ulbricht

(Bearman et al., 2015a). Agent Der-Yeghiayan arrested one of Silk Road's administrators (Cirrus) for her involvement in Silk Road and was able to convince her to cooperate with law enforcement. Der-Yeghiayan assumed Cirrus's account in July, 2013, and began to rise within the Silk Road organization (Bearman et al., 2015b; Jeong, 2015).

Cirrus was not the only person within the Silk Road hierarchy that law enforcement convinced to cooperate with the investigation. Site administrator Curtis Green (online names of Chronicpain and Flush) was arrested as part of the operation. His arrest stemmed from his role as customer service provider for Silk Road. Specifically, he helped resolve drug sale disputes between buyers and sellers on Silk Road. After his arrest, Green agreed to cooperate with law enforcement. As part of that cooperation, he agreed to have his death faked as part of a hit that Ulbricht arranged to have Nob (who was really Agent Force) carry out (Bearman et al., 2015a).

In addition to undercover work and the use of informants, FBI agents were able to track down servers that hosted Silk Road. The first server they found was housed in the Thor Data Center in Iceland. It was recovered in July, 2013. Agents were also able to obtain a list of all computers that had communicated with that server in the last six months (Bearman et al., 2015b). From that initial find, agents were able to discover servers in France, Romania, and the United States shortly thereafter (Bearman et al., 2015b).

The culmination of the operation resulted in the arrest of Ulbricht in a San Francisco library on October 1, 2013. Silk Road was shut down and the Bitcoin in its possession seized (Bearman et al., 2015b). As noted above, Ulbricht was ultimately sentenced to life in prison on May 29, 2015 (Segall, 2015).

After the close of the operation, two agents involved in the operation—Force and Shaun Bridges—were charged with stealing Bitcoin throughout the course of the operation. Both agents were ultimately sentenced to prison, Force receiving a sentence of six and a half years and Bridges receiving a combined sentence of just shy of eight years (Raymond, 2017). Ulbricht raised this issue on appeal of his case, but that appeal was ultimately denied by the appellate court in 2017 (see *United States v. Ulbricht*, 858 F. 3d 71 (2017)).

See also: Bitcoin; Cryptocurrency; Dark Web; Digital Currency; Dread Pirate Roberts (Ulbricht, Ross; 1984–); Drug Trafficking; Silk Road; Tor (The Onion Router)

Further Reading

Bearman, Joshuah, Joshua Davis, and Steven Leckart. 2015a. "The rise & fall of Silk Road, part 1." *Wired*, No. 23.5.

Bearman, Joshuah, Joshua Davis, and Steven Leckart. 2015b. "The rise & fall of Silk Road, part 2." *Wired*, No. 23.6.

Jawaheri, Husam Al, Mashael Al Sabah, Yazan Boshmaf, and Aiman Erbad. 2018. "When a small leak sinks a great ship: Deanonymizing Tor hidden service users through Bitcoin transactions analysis." *Arxiv*. https://arxiv.org/pdf/1801.07501.pdf

Jeong, Sarah. 2015. “The DHS agent who infiltrated Silk Road to take down its kingpin.” *Forbes*, January 14, 2015. https://www.forbes.com/sites/sarahjeong/2015/01/14/the-dhs-agent-who-infiltrated-silk-road-to-take-down-its-kingpin/#11e5394c51fb

Raymond, Nate. 2017. “Ex-agent in Silk Road probe gets more prison time for bitcoin theft.” *Reuters*, November 7, 2017. https://www.reuters.com/article/us-usa-cyber-silkroad/ex-agent-in-silk-road-probe-gets-more-prison-time-for-bitcoin-theft-idUSKBN1D804H

Segall, Laurie. 2015. “Silk Road’s Ross Ulbricht sentenced to life.” CNN, May 29, 2015. https://money.cnn.com/2015/05/29/technology/silk-road-ross-ulbricht-prison-sentence/index.html

OPERATION OLYMPIC GAMES

Operation Olympic Games was a covert operation carried out by the United States and Israel against the Iranian nuclear facility Natanz (named for the city where it is located). To date, however, officials have not acknowledged taking part in this campaign. It was the first known case of cybersabotage, where cyber weapons were used for defense.

In 2006, Iran began a uranium enrichment program in an underground site called Natanz, which they claimed would generate electricity. President George W. Bush claimed that the uranium would not be used for nuclear power but instead for weapons of mass destruction, and he sought to slow down their efforts. He initiated Operation Olympic Games, a cyberwar program against Iranians that would give the United States access to the computer system in Natanz and cause the machines in the nuclear facility to malfunction. The goal was not only to damage Iran’s ability to create nuclear material but also to cause confusion among Iranian scientists working in the plants about why the machines were not working, all without tipping them off that a computer virus was to blame. This would also cause the Iranian government to assume that the scientists responsible for the plant were unable to run the facility (Sanger, 2012).

Operation Olympic Games began in 2007. Officials in the United States built replicas of the centrifuges (the machines that enrich uranium) in Natanz to help them understand how the attack would be carried out. Reconnaissance operations gathered information about the physical layout of the facility. Experts at the U.S. National Security Agency (NSA) wrote the computer “worm” that would eventually be uploaded to the computer system at Natanz and cause havoc on the plant. They were able to get help from spies who inserted bugs into the computers, which also communicated the findings back to the organization (Gates, 2012).

By 2008, the Natanz plant began to falter and the machines in the plant were malfunctioning. The scientists and engineers at the plant did not understand the reasons for the breakdowns. They assumed the underlying cause was faulty parts. As a way to further confuse the Iranian scientists, the attackers introduced different versions of the worm over several years. Because every attack was different, the scientist were unable to understand the reasons for the malfunctioning equipment.

In 2009, President Bush left the White House and explained the program to incoming President Barack Obama, who chose to continue the attacks. Obama expressed concern about setting a precedent that would encourage others to carry out cyberattacks, but he ultimately decided the need to delay Iran's potential for building nuclear weapons was a higher priority (Sanger, 2012). In 2010, Obama asked for more sophisticated attacks on Natanz; working with Israeli officials, the countries decided to target critical centrifuges within Natanz. In order to do this, a new version of the bug was created. The malware disabled almost 1,000 of the 6,000 centrifuges in the plant (Katz, 2010).

The attackers never intended for the malware to go into any systems other than the nuclear facility, but a technician in the facility connected a laptop that had been infected with the worm to the internet, causing the worm to replicate itself outside of Natanz. By the summer of 2010, the bug was available through the internet, and reporters in different media outlets begin to describe a new computer worm that was showing up on computer systems. The newly discovered worm was given the name Stuxnet. For the public, the worm did not cause significant damage.

Even though the worm was now public, President Obama continued to order more cyberattacks on Natanz in an attempt to disable Iran's nuclear programs. Scientists in the plant eventually discovered the malware and quickly contained it, and replaced any damaged machines with new ones. By late 2010 or early 2011, Natanz had fully recovered. Some experts claimed that in the end, Operation Olympic Games may have delayed Iran's ability to develop nuclear weapons by a year or two, but other experts claim that the operation had little effect in the long run (Warrick, 2011).

See also: Cyberwarfare; President and Cybercrime; Worm

Further Reading

Gates, Guilbert. 2012. "How a secret cyberwar program worked." *New York Times*, June 1, 2012. https://archive.nytimes.om/www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html

Katz, Yaakov. 2010. "Stuxnet may have destroyed 1,000 centrifuges at Natanz." *The Jerusalem Post*, December 24, 2010. https://www.jpost.com/Defense/Stuxnet-may-have-destroyed-1000-centrifuges-at-Natanz

Manzo, Vincent. 2013. "Stuxnet and the dangers of cyberwar." *National Interest*, January 29, 2013. nationalinterest.org/commentary/stuxnet-the-dangers-cyberwar-8030

Middleton, Bruce. 2017. *A history of cyber security attacks: 1980 to present*. Boca Raton, FL: CRC Press.

Nakashima, Ellen and Joby Warrick. 2012. "Stuxnet was work of U.S. and Israeli experts, officials say." *Washington Post*, June 2, 2012. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/

Sanger, David E. 2012. "Obama order sped up wave of cyberattacks against Iran." *New York Times*, June 1, 2012. https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-Iran.html.

Warrick, Joby. 2011. "Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack." *Washington Post Foreign Service*, February 16, 2011 http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html

OPERATION PHISH PHRY

In October 2009, over 100 people were charged in the United States (in North Carolina, California, and Nevada) and in Egypt through a law enforcement investigation that began in 2007 and resulted in the largest number of defendants ever charged with the same crime. The inquiry by the Federal Bureau of Investigation (FBI) and Secret Service explored a cyber fraud phishing scam in which the offenders "phished" for sensitive personally identifiable information, including social security numbers, bank account numbers, or drivers' license numbers, by somehow tricking individuals into providing it. This is often done by using fake websites that appear to be genuine. It was estimated that the offenders were able to transfer approximately $1.5 million to accounts held by the offenders.

Operation Phish Phry was based out of Los Angeles and run by the Electronics Crimes Task Force. The task force included a mixture of federal, state, and local law enforcement agents, as well as law enforcement officials from Egypt. The investigation was the first joint cooperative inquiry between these two countries, and it was the largest cybercrime investigation carried out in the United States. In an 86-page indictment, the offenders were accused of stealing information from banks across the United States and stealing financial information from thousands of account holders. More specifically, they were charged with conspiracy to commit wire fraud and bank fraud. Some offenders were also charged with bank fraud, aggravated identity theft, conspiracy to commit computer fraud, unauthorized access to protected computers in connection with fraudulent bank transfers, and domestic and international money laundering.

In this crime, offenders based in Egypt sent e-mails to victims that lured them into visiting what the victims assumed was a site managed by Wells Fargo & Company and Bank of America, two of the largest banks in the United States. The site was actually a sham site controlled by the offenders. When the customers logged on to their accounts, they unknowingly gave their banking account and other personal information to the offenders. The criminals were able to access the victims' bank account and transferred money into outside accounts that they controlled in the United States. The majority of transfers were for an amount between a few hundred dollars and up to $2,000. Offenders in the United States opened the bank accounts that received the money transfers. Some of the diverted funds were then electronically wired to accounts owned by the offenders in Egypt.

Kenneth Joseph Lucas primarily operated the American side of the scheme, with help from Nicole Michelle Merzi and Jonathan Preston Clark, all of whom were residents of California. Lucas, who was 27 years of age, was eventually convicted of 49 counts of bank and wire fraud and sentenced to 13 years in a federal prison. He also received a five-year sentence for a separate conviction related to growing 100 marijuana plants in his home. Merzi, who was 25 years old at the time of the offense, was found guilty of conspiracy, computer fraud, bank fraud, and aggravated identity theft. Others who participated in the scam were Tramond S. Davis, 21 (found guilty of conspiracy), Shontovia D. Debose, 22 (found guilty of conspiracy), Anthony Donnel Fuller, 22 (found guilty of conspiracy and two counts of bank fraud), and MeArlene Settle, 22 (found guilty of conspiracy and two counts of bank fraud).

See also: Phishing; Social Engineering

Further Reading

Federal Bureau of Investigation. "Operation Phish Phry." https://archives.fbi.gov/archives/news/stories/2009/october/phishphry_100709.

Kirk, Jeremy. 2011. "Man sentenced to 13 years in Operation 'Phish Phry.'" *IDG News Service*, June 28, 2011. https://www.networkworld.com/article/2178708/malware-cybercrime/man-sentenced-to-13-years-in-operation--phish-phry-.html

Krebs, Brian. 2009. "33 people arrested as FBI busts international 'phishing' ring." *Washington Post*, October 8, 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/10/07/AR2009100703682.html

McGlasson, Linda. 2009. "'Phish Fry' nets 100 fraudsters." *Bank Info Security*, October 8, 2009. https://www.bankinfosecurity.com/phish-fry-nets-100-fraudsters-a-1846

Stone, Brad. 2009. "FBI indicts dozens in online bank fraud." *New York Times*, October 7, 2009. https://www.nytimes.com/2009/10/08/technology/internet/08phish.html

OPERATION SHROUDED HORIZON

In 2015, the FBI and corresponding agencies in 19 other countries conducted Operation Shrouded Horizon, an investigation of an internet forum called Darkode. Darkode was founded in 2007. It was created—at least in part—by Daniel Placek (Schossow, 2015; Spivak and Daprile, 2015). It was essentially an online marketplace for cybercriminals. Those criminals could buy and sell any number of things used to commit cybercrimes, such as malware, stolen identities, and botnets. It also served as a forum to brainstorm innovative ways to commit cybercrime (Federal Bureau of Investigation, 2015). United States Attorney David J. Hickton described the site as "the most sophisticated English-speaking forum for criminal computer hackers in the world" (United States Department of Justice, 2015).

The investigation started around early 2014 and lasted 18 months (Stevenson, 2015). The FBI indicates it was able to infiltrate Darkode and collect information on its members. As of early 2019, the FBI has not specified how it infiltrated the site. Darkode was a password-protected site. To become a member of Darkode, one had to first be invited by an existing Darkode member. Following that, the prospective member had to validate their membership to the group by presenting the products and services they could contribute to the group (United States Department of Justice, 2015). The Daily Dot—an online publication focusing on internet issues—has indicated that the FBI used informants to infiltrate the site (Turton, 2015). According to article written the day after the FBI published a press release about Operation Shrouded Horizon, two informants helped the FBI infiltrate the site. One of those informants was a source providing information to the journalist writing the article, whose identity was kept anonymous. The other informant was said to be Rory Guidry—one of the people facing criminal charges out of Operation Shrouded Horizon, as noted in the FBI's press release. As of early 2019, the FBI had neither confirmed nor denied that Guidry was an informant in this case. However, information in an at least one other indictment resulting from this investigation indicates an informant was used as part of the investigation into Darkode (see Spivak and Daprile, 2015). Guidry was sentenced May 25, 2016, to a year and a day in prison for attempting to sell information on Darkode, as well as for using a computer to steal money and hack passwords (United States Attorney's Office Western District of Louisiana, 2016).

Operation Shrouded Horizon resulted in the arrest of 28 individuals, 12 of those being charged with crimes in the United States (Stevenson, 2015; United States Department of Justice, 2015). Among those charged in the United States were Daniel Placek, Rory Guidry, and Johan Anders Gudmunds. As noted above, Daniel Placek cocreated the Darkode website. He was charged with creating the site, selling malware on the site, and conspiracy to commit computer fraud. He pleaded guilty to the misdemeanor offense of conspiracy to access a computer without authorization. He was sentenced to two years of probation (Schossow, 2015). As also noted above, Guidry pleaded guilty to charges arising from his involvement with Darkode and was sentenced to a year and a day in prison. Gudmunds—a Swedish resident who went by the name Mafia online—was charged with being the administrator of Darkode. He was also charged with operating a botnet that stole data from computers on approximately 200,000,000 occasions (United States Department of Justice, 2015). As of early 2019, Gudmunds appears to be a fugitive (Lord, 2016).

While several members were arrested and charged with crimes arising from their involvement in Darkode, it appears that the operation did not secure the arrest of most of Darkode's staff or its senior members. Darkode was back online just two weeks after arrests were made as part of Operation Shrouded Horizon (Stevenson, 2015). On its place-holding site, darkcode.cc, the following message appeared shortly after the arrests: "Most of the staff is intact, along with senior members. It appears the raids focused on newly added individuals or people that have been retired from the scene for years" (Clark, 2015).

A new administrator, going by the name Sp3cial1st, indicated that security measures were going to be significantly improved with the new iteration of the Darkode website. Each member of the new Darkode site would be required to have their own personal onion—software that conceals the internet use of the user. Members would also have their accounts authenticated through the use of blockchain technology (Clark, 2015; Pauli, 2015). This attempt to revive Darkode was short-lived and ultimately did not pan out (Cox, 2016). In late 2016, another relaunch of Darkode was attempted by former Darkode members Six and Node. Their version planned to be more restrained than the original Darkode. Posting personally identifying information of victims (credit card numbers, social security numbers, etc.) would be banned, as well as the posting of functional malware. It seems as though the purpose of reviving the site was more for past members to reunite (Cox, 2016). It is unclear how successful that version of Darkode has been.

See also: Bots and Botnets; Federal Bureau of Investigation; Hacker and Hacking; Identity Theft; Lizard Squad; Malware

Further Reading

Clark, Liat. 2015. "Hacker forum Darkode is back and more secure than ever." *Wired*, July 28, 2015. https://www.wired.co.uk/article/darkode-back-and-more-secure

Cox, Joseph. 2016. "Malware exchange busted by the Feds relaunches, at least in name." *Motherboard*, December 19, 2016. https://motherboard.vice.com/en_us/article/pgkwvv/darkode-brand-relaunches

Federal Bureau of Investigation. 2015. "Cyber criminal forum taken down." https://www.fbi.gov/news/stories/cyber-criminal-forum-taken-down

Lord, Rich. 2016. "FBI director says Pittsburgh-based cybercrime busts send key message." *Pittsburg Post-Gazette*, January 13, 2016. https://www.post-gazette.com/local/city/2016/01/13/FBI-director-makes-stop-in-Pittsburgh/stories/201601130218

Pauli, Darren. 2015. "Cybercrime forum Darkode returns with security, admins intact." *The Register*, July 28, 2015. https://www.theregister.co.uk/2015/07/28/darkode_returns/

Schossow, Breann. 2015. "Glendale man who helped create a malware marketplace gets probation." *Journal Sentinel*, December 9, 2015. http://archive.jsonline.com/news/crime/glendale-man-who-helped-create-a-malware-marketplace-gets-probation-b99630425z1-361366181.html/

Spivak, Cary and Lucas Daprile. 2015. "Placek to plead guilty for role in creating Darkode hacker marketplace." *Journal Sentinel*, July 31, 2015. http://archive.jsonline.com/business/placek-to-plead-guilty-for-role-in-creating-darkode-hacker-marketplace-b99548498z1-320345691.html/

Stevenson, Alastair. 2015. "It only took 2 weeks for the world's most dangerous hacking forum to get back online after the FBI shut it down." *Business Insider*, July 28, 2015. https://www.businessinsider.com/darkode-admin-returns-with-new-and-improved-hacking-site-2015-7

Turton, William. 2015. "How the FBI may have infiltrated Darkode." *The Daily Dot*, July 16, 2015. https://www.dailydot.com/crime/darkode-fbi-informant-kms/

United States Attorney's Office, Western District of Louisiana. 2016. "Opelousas man sentenced to a year in prison for role in major computer hacking forum." United States Attorney's Office, Western District of Louisiana, May 25, 2016. https://www.justice.gov/usao-wdla/pr/opelousas-man-sentenced-year-prison-role-major-computer-hacking-forum

United States Department of Justice. 2015. "Major computer hacking forum dismantled." July 15, 2015. https://www.justice.gov/opa/pr/major-computer-hacking-forum-dismantled

P

PASSWORD

A password is an alphanumeric string of characters used to access software, an online service, computer network, or similar platform. Passwords are a security measure that developers put in place to permit only authorized users to access the platform in question. If a cybercriminal is able to discover a password, they can gain unauthorized access to the platform in question. Accordingly, cybercriminals have developed several techniques to discover passwords.

One method used by cybercriminals to discover passwords is the use of malware. One type of software that cybercriminals may attempt to surreptitiously install on a victim's computer is a password sniffer. A password sniffer monitors and records all passwords sent and received by a computer. Another type of software a cybercriminal could use is a keystroke monitor. A keystroke monitor records every keystroke made on a computer's keyboard. A cybercriminal can then analyze the record of keystrokes to find alphanumeric strings within the record that could possibly be a password.

Another method cybercriminals can use is phishing or other social engineering methods. Cybercriminals use such attacks to deceive victims and induce them to divulge their password or other personally identifying information that may enable them to discover the victim's password. These attacks generally come in the form of e-mails, telephone calls, or other non-face-to-face communication.

Deception is not the only means by which a cybercriminal can discover a password directly from the victim. A cybercriminal can simply observe a victim and watch them type their password in. To avoid detection, the cybercriminal has to observe in such a way that does not alert the victim or others around them. The cybercriminal will need to have access to the area in which the computer or other electronic devices is located in order to use this method. Observing in a public area—such as watching someone input their PIN number when using a credit card in the grocery line, watching someone input their social media password on their phone while at the park, or watching someone input their e-mail password on a computer at the public library—may be easier for a cybercriminal, as no special permission will generally be required to be at those locations. This is not to say that a cybercriminal cannot obtain a password through observation of private locations. A coworker or an authorized visitor is just as able to look over a victim's shoulder as they input a password on their work computer as a cybercriminal in a public library is able to look over someone's shoulder when they input a password on a public computer. There are additional ways a cybercriminal may be able to observe a victim's password in private locations. For example, if the victim writes down their password on a sticky note and puts on their monitor, under their keyboard, in a drawer, and so on, a cybercriminal may be able to see that and simply write it down.

A cybercriminal may simply try to guess a password to gain unauthorized access. Those guesses may be educated guesses, using names and other words that have significance to the victim. A cybercriminal can find such information by browsing a victim's social media pages and other public information. A cybercriminal may also use a brute force attack. A brute force attack is where a cybercriminal—generally through the use of software—attempts to input numerous different passwords in rapid succession until the correct password is ultimately guessed.

There are measures that can be taken to lessen the likelihood of having one's password guessed by cybercriminals. As noted above, cybercriminals may use personal information they find online when attempting to discover a victim's password. Thus, avoiding the use of personal information in a password can lessen the likelihood of that password being discovered. Additionally, the use of passwords that are not actually words can help, as well as making the password long and using nonconsecutive symbols in the password. It is also recommended that the same password not be used for multiple computers or online services (Barrett, 2017; McAfee, 2011; Symantec, 2019).

See also: Keystroke Monitoring; Malware; Phishing; Sniffer; Social Engineering; Vulnerability

Further Reading

Barrett, Brian. 2017. "Take these 7 steps now to reach password perfection." *Wired*, December 9, 2017. https://www.wired.com/story/7-steps-to-password-perfection/

McAfee. 2011. "15 tips to better password security." *McAfee*, June 29, 2011. https://securingtomorrow.mcafee.com/consumer/family-safety/15-tips-to-better-password-security/

Symantec. 2019. "Help secure your accounts with these strong password tips." *Symantec*. https://us.norton.com/internetsecurity-how-to-how-to-secure-your-passwords.html

PAYLOAD

In regard to malware, the payload is the part of the malware that causes harm. There can be other components of malware that assist in the execution of the payload. The type of harm inflicted by a given piece of malware will vary depending on the goal of the cybercriminal distributing the malware. A common objective is the theft of information. The information stolen may be personally identifying information that enables a cybercriminal to steal money from the victim. Spyware is one type of malware that enables a cybercriminal to obtain this information. Spyware is any malware that collects data and transmits it back to the cybercriminal. Some specific types of spyware are sniffers and keystroke monitors. Sniffers monitor the online information that goes through a server, and keystroke monitors keep a log of all keys pressed on a keyboard of a given computer and send that information back to a cybercriminal.

In addition to using malware for financial gain, a cybercriminal may also want to use malware to inflict financial or other harm on a victim. This can be done in several ways. A cybercriminal can launch a DDoS attack against a website, rendering the website useless for a period of time. This can result in financial loss for the website targeted. Not only might the website miss out on revenue it might otherwise have generated had the website remained operational, but customer confidence in the business that owns the website may drop as a result of the attack, causing a drop in the valuation of that business and its stock prices (Bose and Leung, 2014; Goel and Shawky, 2009; Pirounias et al., 2014; Spanos and Angelis, 2014). Malware might also be used to cause a computer to be inoperable, rendering it useless. In some instances, malware might cause physical damage to property other than the infected computer itself. In 2010, the centrifuges at Iran's Natanz nuclear facility suffered damage through the Stuxnet computer worm. The worm caused this damage by directing the centrifuges to rotate faster than they were supposed to (Warrick, 2011).

Another harm that can be inflicted via malware is having one's computer remotely controlled by a cybercriminal. This is done through the use of bots. Although having surreptitious control of another computer can enable a cybercriminal to steal information from that computer, it also enables a cybercriminal to use the infected computer for other criminal purposes, such as launching a DDoS attack using a network of computers infected with bots (i.e., a botnet).

There are other aspects of malware that can enable a cybercriminal to execute the payload. For example, a Trojan horse is a mechanism that hides malware within another seemingly innocuous piece of software. The Trojan horse is not the payload, but it does assist in the delivery of the payload. Rootkits are designed to hide the existence of malware on an infected computer. The rootkit itself does not cause the harm, but it reduces the likelihood that the payload will be discovered and removed. A logic bomb is designed to execute the payload of malware upon the occurrence of some event. Again, the logic bomb does not cause the harm, but it assists in the execution of the payload, enabling it to be triggered at times strategic to the cybercriminal.

See also: Bots and Botnets; Distributed Denial-of-Service Attack (DDoS); Economy, Effects on; Identity Theft; International Issues; Keystroke Monitoring; Logic Bomb; Malware; Personally Identifying Information; Rootkit; Sniffer; Spyware; Trojan Horse; Vandalism

Further Reading

Bose, Indranil, and Alvin Chung Man Leung. 2014. "Do phishing alerts impact global corporations? A firm value analysis." *Decision Support Systems* 64: 67–78.

Goel, Sanjay, and Hany A. Shawky. 2009. "Estimating the market impact of security breach announcements on firm values." *Information & Management* 46: 404–410.

Pirounias, Sotirios, Dimitrios Mermigas, and Constantinos Patsakis. 2014. "The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study." *Journal of Information Security and Applications* 19: 257–271.

Spanos, Georgios, and Lefteris Angelis. 2016. "The impact of information security events to the stock market: A systematic literature review." *Computers & Security* 58: 216–229.

Warrick, Joby. 2011. "Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack." *Washington Post*, February 16, 2011. http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html

PEN REGISTER

A pen register, or sometimes called a dialed number recorder, is a device that records all outgoing phone calls from a particular line or telephone number. Pen registers can track phone numbers that are dialed from that phone or number, the time that the call was made, and the length of the call. More recent technology called triggerfish and stingrays can track signals given off by cell phones to identify the numbers called from that device. In some cases, the content of any text messages that were sent from that phone can also be tracked. The information collected from pen registers, triggerfish, and stingrays can show a lot about a person, including not only whom they call but also the websites they visit, and information on social media.

The pen register can also track any other device that performs similar functions, such as programs designed to monitor internet usage. Another device, called a trap and trade device, can identify incoming calls to the home.

The U.S. Federal Code defines device pen register as a device that

> records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

There are multiple differences between a pen register and a wiretap. One is that the pen register only gathers information on incoming and outgoing calls, whereas the wiretap provides information on the content of the person who called. A pen register can be used alongside a wiretap in order to gather additional evidence against an offender. Triggerfish and stingray technology can track phone calls made from a cellular phone and the content of text messages. In all cases, police must show probable cause that a crime has been committed or will be committed in order to obtain a warrant for a wiretap, a triggerfish, or a stingray device. The standard is lower for a pen register. The agent only has to show that the information collected is relevant to an ongoing criminal investigation.

It should be noted that a pen register shows only a general number called; it cannot identify the specific person that picks up the phone on the other end of the line. Nonetheless, reports show that the use of pen registers by federal law enforcement has rapidly increased in recent years because it does not require a search warrant.

In 1986, Congress passed the Electronic Communications Privacy Act that placed limits on an officer's ability to access a suspect's electronic communications. Some provisions of this law were known as the Pen Register Act by which Congress placed limits on use of pen registers by both law enforcement agents and private individuals. Any law enforcement agent seeking to use a pen register must be granted permission to use one by a court through a warrant issued by a judge. The judge must ensure that the information sought by the pen register is somehow related to an ongoing criminal investigation.

The laws for pen registers changed after the terrorist attacks of September 11, 2001, when Congress passed the USA PATRIOT Act. At the time, they sought to gather information on which numbers were calling others. This was permitted until 2015, when President Barack Obama ordered the program to be stopped, which occurred when the USA Freedom Act was passed (Obama, 2015). The PATRIOT Act also altered the definition of a pen register. It now includes all devices that provide a similar function with internet communications, which means that police can gather information on outgoing calls from all devices, not just a phone. Any law enforcement individual can ask a service provider to grant them access to a suspect's phone records so the police can see whom the defendant called. A law enforcement agent is able to see the header information from an e-mail, the addresses of all e-mails that are sent; the e-mails of people who sent e-mails; the time of day the e-mail is sent and how large it is; and the content. For the internet, the investigator can see the IP address of all websites accessed; the time of day the site was accessed; and how long a person was on that site.

The U.S. Supreme Court has upheld the constitutionality of pen registers in *Smith v. Maryland*, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979). The justices decided that that the use of a pen register is not an invasion of an individual's right to privacy. The case revolved around robbery victim Patricia McDonough, who received telephone calls from Michael Lee Smith, the man who claimed to be the person who robbed McDonough. During one of the calls, the man asked McDonough to step out of the home and onto the porch. As she did, she was able to identify the car that she had previously described to the police as the one that belonged to the robber. The police discovered that the registered owner of the car was Smith. The police then approached the telephone company and asked to install a pen register that would trace all numbers that were dialed from Smith's telephone. The register provided proof that a call was made from Smith's residence to McDonough's telephone. Based on this and other evidence, the police were able to obtain a search warrant for Smith's home, where they found a telephone book that was open to the page that listed the victim's address. Police arrested Smith.

The Supreme Court held that the pen register was installed on the telephone company's property, so Smith's privacy was not being invaded. Further, Smith did not expect privacy in the telephone numbers he dialed. Any phone number that a caller dials must be processed through the telephone company, which also keeps records of calls made for billing purposes. The court ruled that the victim did not have an expectation of privacy when he dialed telephone numbers. Thus, the court ruled that the use of the pen register was not a "search" under the Fourth Amendment, so a search warrant was not required for its installation.

In 2018, Federal Bureau of Investigation (FBI) agents attempted to gather evidence against President Donald Trump's personal attorney and vice-president of the Trump Organization, Michael Cohen. In order to know who he was calling, agents placed a pen register on his phones. Unlike a wiretap that allows officers to know the content of all calls coming in and out of the home, the pen register only shows who he called. They found that Cohen called someone in the White House, but they were unable to know who that was or what was discussed.

See also: Federal Bureau of Investigation; Privacy

Further Reading

Baker, Stewart A., and John Kavanagh. 2005. "Patriot debates: Experts debate the USA Patriot Act." Chicago, IL: American Bar Association.

Bump, Philip. 2018. "The very big difference between a wiretap and how the feds tracked Michael Cohen." *Washington Post*, May 4, 2018. https://www.washingtonpost.com/news/politics/wp/2018/05/04/the-very-big-difference-between-a-wiretap-and-how-the-feds-tracked-michael-cohen/?utm_term=.53e982548485

Mukasey, Michael B. 2009. "Intelligence averts another attack." *Wall Street Journal*, October 1, 2009. https://www.wsj.com/articles/SB10001424052748704471504574446970300914330

Obama, Barack. 2015. "Statement by the President on the USA FREEDOM Act." The White House, June 2, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/06/02/statement-president-usa-freedom-act

Shaw, Thomas J. 2011. *Information security and privacy: A practical guide for global executives, lawyers and technologists*." Chicago, IL: American Bar Association.

Valentino-DeVries, Jennifer. 2014. "Sealed court files obscure rise in electronic surveillance; Law enforcement requests to monitor cellphones are routinely sealed—and stay that way." *Wall Street Journal*, June 2, 2014. https://www.wsj.com/articles/sealed-court-files-obscure-rise-in-electronic-surveillance-1401761770

PEOPLE'S LIBERATION ARMY UNIT 61398

China has been suspected of committing numerous cyberattacks against foreign governments and businesses. Indeed, China appears to be the most prolific country in terms of cyberattacks. From 2006 to early 2019, China is believed to have carried out over 100 cyberattacks against foreign entities. In a number of these incidents, it is believed that the PLA specifically orchestrated the attacks (Center for Strategic and International Studies, 2019). In 2013, a report was released identifying Unit 61398 of the PLA as at least one of the groups within the PLA carrying out cyberattacks (Mandiant, 2013). For years, China denied responsibility for these cyberattacks that are believed to be perpetrated by them, or that China even had a division of the PLA that was dedicated to such activities. In 2015, China did admit to the existence of cyberwarfare units within the PLA. This revelation was made in the *Science of Military Strategy*—a publication of the PLA (Osborne, 2015).

Unit 61398 appears to be designed specifically to conduct cyberespionage against foreign businesses. English-speaking countries in particular appear to be targeted by the unit. Members of the unit are required to be fluent in English, and 87 percent of the businesses victimized by the unit were located in English-speaking countries. The businesses hit are in industries that China has identified as important to their economic growth. It was estimated that the unit has hundreds, and possibly thousands, of members. The information stolen by the unit includes technological intellectual property (blueprints, etc.) and business information (business plans, contact lists, etc.).

There are various methods the PLA has used to conduct cyberespionage. In 2010, officials in the United Kingdom indicated the members of the PLA were approaching businessmen from the United Kingdom at trade fairs and similar events, trying to give them free flash drives and similar items. The flash drives contained spyware (Center for Strategic and International Studies, 2019). In 2015, it was discovered that microchips were being installed on servers manufactured in China that allowed the activity on those servers to be monitored. Those servers were being used in the computer networks of foreign government agencies and corporations located in foreign countries. It is believed that the PLA installed those microchips to allow China to gather data on those entities (Robertson and Riley, 2018). In many instances, the cyberattacks may not necessarily be sophisticated. However, the sheer volume of attacks renders businesses and other entities vulnerable (Osborne, 2014).

There have been a few members of Unit 61398 that have been identified. In the original report identifying Unit 61398 as a cyberattack unit of the PLA, three members were identified by their online names: UglyGorilla, DOTA, and SuperHard (Mandiant, 2013). On May 19, 2014, the United States indicted five members of Unit 61398 for computer fraud, identity theft, theft of trade secrets, economic espionage, and other cybercrimes. Those five are Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui (United States Department of Justice, 2014). Wang Dong has been identified as UglyGorilla—one of the hackers mentioned in the initial report on Unit 61398. The other four suspects had aliases as well: Sun Kailiang went by Jack Sun, Wen Xinyu went by WinXYHappy, Huang Zhenyu went by hzy_lhx, and Gu Chunhui went by KandyGoo (Martosko, 2014). The organizations that were victims of the cyberattacks that led to these charges were Westinghouse, SolarWorld, U.S. Steel, Allegheny Technologies, the United Steelworkers Union, and Alcoa. The indictment of these five marked the first time in the United States that criminal charges had been filed against state actors from another country for cybercrime (United States Department of Justice, 2014). China denied that the named suspects engaged in the crimes alleged by the United States. As all five suspects reside in China, it seems highly unlikely that they will be extradited to the United States (Wee, 2014). The United States identified one of the senior officials in the PLA behind cyberattacks in 2018: Major General Liu Xiaobel (Gertz, 2018). As of early 2019, Xiaobel has not been charged with any crimes in the United States.

See also: China; Hacker and Hacking; Identity Theft; Political Uses; Spyware

Further Reading

Center for Strategic and International Studies. 2019. "Significant cyber incidents.". https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

Gertz, Bill. 2018. "China cyber spy chief revealed." *Washington Times*, March 28, 2018. https://www.washingtontimes.com/news/2018/mar/28/liu-xiaobei-heads-chinas-us-hacking-operations/

Mandiant. 2013. "APT1: Exposing one of China's cyber espionage units." Mandiant. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Martosko, David. 2014. "Meet 'UglyGorilla,' 'KandyGoo' and 'WinXYHappy'—America's newest most wanted: Criminal charges brought against Chinese Army officials who hacked U.S. firms—But is there any real hope of prosecuting them?" *The Daily Mail*, May 19, 2014. https://www.dailymail.co.uk/news/article-2632719/US-Official-China-cited-cyber-espionage-case.html

Osborne, Charlie. 2014. "FBI chief compares Chinese hackers to 'drunk burglars.'" *ZDNet*, October 6, 2014. https://www.zdnet.com/article/fbi-chief-compares-chinese-hackers-to-drunk-burglars/

Osborne, Charlie. 2015. "China reveals existence of cyber warfare hacking teams." *ZDNet*, March 20, 2015. https://www.zdnet.com/article/china-reveals-existence-of-cyber-warfare-hacking-teams/

Robertson, Jordan and Michael Riley. 2018. "The big hack: How China used a tiny chip to infiltrate U.S. companies." *Bloomberg Businessweek*, October 4, 2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

United States Department of Justice. 2014. "U.S. charges five Chinese military hackers for cyber espionage against U.S. corporations and a labor organization for commercial advantage." May 19, 2014. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

Wee, Sui-Lee. 2014. "China confronts U.S. envoy over cyber-spying accusations." *Reuters*, May21,2014.https://www.reuters.com/article/us-china-usa-espionage/china-confronts-u-s-envoy-over-cyber-spying-accusations-idUSBREA4J03D20140521

PERSONAL DATA NOTIFICATION AND PROTECTION ACT OF 2017

The Personal Data Notification and Protection Act was a proposal for a new law that was presented to the House of Representatives in the 115th Congress that would establish a national system for notifying victims of data breaches. The law was considered by members of the House of Representatives but ultimately not passed into law.

U.S. Representative James R. Langevin (D-RI), chair of the Congressional Cybersecurity Caucus, first proposed a bill that would require businesses and organization to notify customers or clients if their personal information may have been (or was) hacked on March 26, 2015. Called the Personal Data Notification and Protection Act of 2015, it was sent to the House Judiciary Committee, followed by the Subcommittee on the Constitution and Civil Justice but was not passed.

When this early version of the bill was introduced in 2015, it had the support of President Barack Obama and was even considered to be a priority for the administration. He discussed it in his January 20, 2015, State of the Union address when he said:

> No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids. So we're making sure our Government integrates intelligence to combat cyber threats, just as we have done to combat terrorism. And tonight I urge this Congress to finally pass the legislation we need to better meet the evolving threat of cyber attacks, combat identity theft, and protect our children's information. That should be a bipartisan effort. If we don't act, we'll leave our Nation and our economy vulnerable. If we do, we can continue to protect the technologies that have unleashed untold opportunities for people around the globe. (Obama, 2015)

In 2017, hackers accessed personal information for millions of customers of Equifax, a major credit reporting agency. The hackers were able to view customers' Social Security numbers, birthdays, driver's licenses, and credit card information. Although the breach continued from mid-May until July, Equifax did not announce the breach until September. Without that knowledge, victims did not take precautions to protect their information, increasing the chances of additional cybercrimes.

In discussing the events of the Equifax breach, Representative Langevin indicated that had his original bill been passed, victims in this case would have been notified much quicker and been able to take preventative action to protect themselves. In response, Langevin again proposed the Personal Data Notification Act on September 18, 2017. Langevin noted that the company had done a "terrible job communicating about the breach to date" (Uchill, 2017). While many states at that time had existing laws that required some kind of notification to customers if a data breach occurred, many other states did not. In addition, the laws across those states were very different, and the standards among the state laws differed. The proposed federal legislation would set a consistent standard across the nation for notification of data breaches.

Members of the Judiciary Committee and the Subcommittee on Digital Commerce and Consumer Protection debated the bill. The general purpose or intent of the bill was to establish a national data breach notification standard. Under the proposal, any businesses that used, accessed, stored, disposed of, or collected sensitive personally identifiable information would be required to notify their customers whose personal information may have been accessed or acquired after a security breach. Examples of personal information that would be covered under the bill include Social Security numbers, passport numbers, financial account numbers, or credit card numbers. Notification of clients and customers would not be required if there was no risk of harm to the individuals.

When a company discovers a possible breach of their computer systems, officials would be required to notify their clients or customers within 30 days of the discovery. This could be done by a letter, a phone call, or even an e-mail that would provide the client or customer with a general description of the information that was, or may have been, accessed. In addition to the general notification, the business or agency must give the client or customer with a toll-free phone number that they could use to contact someone who has more specific details about the breach and the information that may have been stolen. If the breaches may have affected over 5,000 customers, the company or organization would have to notify major media outlets. In addition to all of this, the affected business or organization would also have to notify credit reporting agencies of the possible breach.

Another provision in the proposal would require officials in the DHS to establish a federal agency that would gather information on all security breaches that are discovered by companies and organizations. Any business who discovers a breach must notify DHS so information on that breach could be detailed and collected. Some data breaches were considered to be more serious and had to be reported to the U.S. Secret Service, the FBI, and the Federal Trade Commission (FTC). This would be breaches of databases that included information on over 500,000 individuals, a federal government database, or a database that included information on federal employees who work in law enforcement or national security.

Officials in a business or organization that fail to follow these new rules on breaches may be found guilty of violating federal laws regarding unfair and deceptive acts. Any cybercriminals who hack into these databases may also be charged with various state-level offenses if the attorney general of that state has reason to believe that victims in that state may have been affected by the official's failure to report the breach. The state attorney general also has the option to bring civil charges against company officials as a way to force them to comply with the rules established here. This can include civil penalties of up to $1,000 per day per customer whose personal information was, or may have been, accessed in the breach, with a maximum fine of $1 million per breach.

While many company officials showed their support for the proposed bill, others were less supportive. Some of their concerns revolved around the definition of personal identification. Under the bill, passwords were included as personally identifiable information, which, according to some executives, generally do not result in a security threat. They noted that that a breach of passwords should not trigger the notification process. Other executives indicated that the 30 day period for notifying victims after a breach was too short for the company to fully investigate a possible breach and discover the full extent of the damage, if any. Yet other opponents argued that the states already had laws, and they should be the ones that oversaw these events instead of the federal government. Finally, opponents also complained that the proposed law only covered personal information that was included in electronic format and ignored paper forms.

See also: Equifax Breach; Personally Identifying Information; President and Cybercrime

Further Reading

HR 1704. "Personal Data Notification and Protection Act of 2015." Congress.Gov. https://www.congress.gov/bill/114th-congress/house-bill/1704

HR 3806. "Personal Data Notification and Protection Act of 2017." Congress.Gov. https://www.congress.gov/bill/115th-congress/house-bill/3806

Mims, Christopher. 2017. "After Equifax, should the government force companies to report hacks? Companies like Equifax don't like you knowing they've been hacked—but it would be better for consumers and businesses if they were quicker to report it." *Wall Street Journal*, September 24, 2017. https://www.wsj.com/articles/should-the-u-s-require-companies-to-report-breaches-1506254402

Obama, Barack. 2015. "Address before a joint session of the Congress on the State of the Union." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, January 20, 2015. http://www.presidency.ucsb.edu/ws/?pid=108031

Uchill, Joe. 2017. "Dem reintroduces breach notification law in Equifax wake." *The Hill*, September 18, 2017. http://thehill.com/policy/cybersecurity/361164-dem-reintroduces-national-breach-notification-law

PERSONALLY IDENTIFYING INFORMATION

Personally identifying information is any information that can be used to as a means of identifying an individual. This information can be used by cybercriminals to defraud or otherwise victimize the individual whose information was obtained. Personally identifying information includes information that can be used to directly identify someone, such as an individual's name, date of birth, and social security number. It also includes contact information for an individual, such as a phone number, physical address, or e-mail address. Demographic information, such as race and sex, would be included as well. In the cyber context, online account information is also personally identifying information. This includes the login credentials (username and password) for financial, social media, and other online accounts. Any information that could be used to answer a security question for one of those accounts (e.g., your mother's maiden name, the name of your first pet, the color of your first car) also becomes personally identifying information (LifeLock, 2019).

There are several ways a cybercriminal might use the personally identifying information of others. Generally speaking, this information is used by cybercriminals for financial gain. One way this can be done is through identity theft. Armed with the proper personally identifying information of a victim, a cybercriminal can pose as the victim to either access existing financial accounts of the victim or to start new accounts under the victim's identity. Both result in financial loss to the victim. Some cybercriminals amass the personally identifying information of numerous victims and then sell that information online to other cybercriminals via an online black market website.

There are several ways a cybercriminal can collect the personally identifying information of a victim. A common method is phishing—posing as someone you are not for the purpose of convincing a victim to divulge personally identifying information to you. This is often done via e-mail. Phishing can be used to exponentially obtain the personally identifying information of victims. Once a cybercriminal is able to use personally identifying information to compromise the e-mail or other electronic communication account of one victim, that cybercriminal can then spoof e-mails to the victim's contact list, posing as the victim. If these additional phishing attacks are successful, the cybercriminal not only has more potential victims to profit from, but they can repeat the cycle, sending spoofed e-mails to the new victims' contact lists.

There are physical methods of obtaining personally information as well, such as scavenging (e.g., looking for information on documents that have been thrown in the garbage). Another avenue cybercriminals can use is the collection of information that is publicly available. Gathering data in that fashion can be time-consuming. There are data-aggregation websites that compile publicly available data and make it available to others—usually for a fee. Websites that provide data like this are not violating the law, as the data provided is publicly available, and the website is simply saving others the hassle of compiling that data (Cox, 2018). Nonetheless, if a cybercriminal uses that data to ultimately commit identity theft or some other crime, that would clearly be illegal.

A number of things can be done to prevent personally identifying information from falling into the hands of cybercriminals. This includes limiting the amount of information shared on social media, and only divulging personally identifying information to entities that need the information and who you trust to keep it private (LifeLock, 2019). Businesses must also worry about their data collection policies as cybercriminals may target them to collect the personally identifying information of numerous people in one attack. One recommendation to businesses by the Federal Trade Commission (2016) is to only collect and retain data that is absolutely necessary to operate the business, thus minimizing the amount of information cybercriminals might be able to obtain should they be able to breach the business's security measures. A nondigital way that both individuals and businesses can prevent personally identifying information from falling into the hands of cybercriminals is the proper disposal of physical records that contain such information. This requires that records are not just thrown away but also in some way destroyed (e.g., shredded) before they are thrown away (Federal Trade Commission, 2016; LifeLock, 2019). If this is done, a cybercriminal engaging in scavenging will not be able to obtain information from the trashed records.

See also: Financial Crimes; Identity Theft; Password; Phishing; Scavenging; Spoofing

Further Reading

Cox, Kate. 2018. "It's creepy, but not illegal, for this website to provide all your public info to anyone." Consumer Reports, May 4, 2018. https://www.consumerreports.org/consumerist/its-creepy-but-not-illegal-for-this-website-to-provide-all-your-public-info-to-anyone/

Federal Trade Commission. 2016. "Protecting personal information: A guide for business." https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

LifeLock. 2019. "What is personally identifiable information (PII)?" LifeLock. https://www.lifelock.com/learn-identity-theft-resources-what-is-personally-identifiable-information.html

PHARMING

Pharming is a cyberattack wherein a cybercriminal will create a mimicked version of a legitimate website. This is done to deceive victims into divulging personally identifying information to the cybercriminal via the spoofed website, believing they are providing it to the operators of the legitimate website. Once a cybercriminal obtains that information, they can use it to commit identity theft, theft, and other financial crimes.

There are several ways pharming can take place. One method cybercriminals might use is typosquatting—using a domain name that it one character different from a legitimate domain name. This is done to try and catch users of a legitimate website that are careless when entering the domain name (Brody et al., 2007). If the website at a typosquatting domain name spoofs the legitimate website, a user that is unaware of the fact they made a typo might enter their personal information (e.g., login credentials, bank account number). While this is a method cybercriminals could use to conduct a pharming attack, it does not appear that this method is used often. One study found that less than 3 percent of the typosquatted websites were associated with cybercrime (Ducklin, 2018). The lack of pharming via typosquatted websites may be due to the scarcity of typosquatting domain names. Engaging in criminal activity via such a domain name may require a cybercriminal to ultimately abandon that domain name, and the profit that can come from it. Indeed, 15 percent of the typosquatted websites visited in the study bombarded visitors with ads and popups—a potential means of generating revenue.

Another method used to pharm is through the use of malware. To enable pharming, malware can be designed to affect the functionality of a computer's web browser. Specifically, the malware will cause a computer to direct the user to the cybercriminal's spoofed website instead of the actual website typed into the web browser (Brody et al., 2007; Kaspersky, 2019). A pharming attack using this method was carried out in 2007. In that attack, cybercriminals designed malware that would redirect victims to spoofed versions of bank account websites. The malware would redirect victims to spoofed bank websites if they attempted to visit one of over 50 different bank websites. Once login credentials were entered by victims, they were redirected to the legitimate bank websites and logged in with the credentials they have provided to the cybercriminals, thus leaving them unaware they have been hit by a pharming attack (Kirk, 2007).

Cybercriminals may attack a DNS server instead of a computer to carry out a pharming attack. By using DNS spoofing, cybercriminals can cause a DNS server to direct correctly entered domain names to internet protocol (IP) addresses that do not correspond to those domain names. This can send victims to a spoofed website (Brody et al., 2007; Kaspersky, 2019). This method of pharming can be more difficult to protect against. In instances of pharming via typosquatting, users can take precautions and make sure to type carefully when visiting websites where they will be asked to enter sensitive information. In instances of pharming via malware, users can keep their antimalware software up to date and engage in safe web-browsing practices to help avoid having pharming malware downloaded onto their computers. With DNS spoofing, these precautions may be insufficient, as the attack is against a DNS server, which the user will not generally have control over (Kaspersky, 2019).

While some forms of pharming may be more difficult to protect against, there are still measures that can be taken to mitigate the risk of falling victim to a pharming attack. In addition to the precautions mentioned above, users can pay attention to the websites they visit. If the website does not appear the way it normally does (e.g., the design is different, the address bar looks different, the site asks for information it does not normally ask for), it is possible the website is part of a pharming attack (Kaspersky, 2019). The majority of pharming attacks spoof the websites of financial institutions. Accordingly, there are additional precautions those institutions might take to protect against pharming attacks. For example, banks may implement a system whereby customers choose a personal image that is to appear whenever they attempt to log in to their account. If the image does not appear, it is an indication that the website the customer accessed may not be legitimate, and they should not enter their login credentials (Brody et al., 2007).

See also: Cybersquatting; Domain Name System Cache Poisoning; Financial Crimes; Identity Theft; Malware; Personally Identifying Information; Phishing; Spoofing

Further Reading

Brody, Richard G., Elizabeth Mulig, and Valerie Kimball. 2007. "Phishing, pharming and identity theft." *Academy of Accounting and Financial Studies Journal* 11, 3: 43–56.

Ducklin, Paul. 2018. "Typosquatting—What happens when you mistype a website name?" Sophos. https://nakedsecurity.sophos.com/typosquatting/

Kaspersky. 2019. "What is pharming?" Kaspersky. https://usa.kaspersky.com/resource-center/definitions/pharming

Kirk, Jeremy. 2007. "Pharming attack targeted bank customers worldwide." *PCWorld*, February 22, 2007. https://www.pcworld.com/article/129270/article.html

PHISHING

Phishing is a type of cyberattack wherein the perpetrator sends an electronic communication to a victim, purporting to be someone they are not. Phishing is a common method of social engineering—obtaining personally identifying information of another through deception. By pretending to be someone else, a cybercriminal may be able to convince a victim to divulge personally identifying information. A cybercriminal might pretend to be a business or government agency, claiming to need the victim's information for official purposes. They might also pretend to be a friend or family member, using that trust to encourage a victim to divulge personal information. If a phishing attack is successful, a cybercriminal can then use the personally identifying information they obtain to commit theft or other financial crimes.

Phishing can occur by any means of electronic communications. However, the vast majority of phishing appears to occur via e-mail (Verizon, 2018). Other methods include text message, social media message, or phone call—referred to as "vishing" (Vanian, 2019). Phishing can be used to gain one individual's personal information. It can also be used to gain information that would permit the cybercriminal to access the computer network of a business, government agency, or other organization. When a phishing scheme is set up to target a specific victim, it is referred to as spear phishing. When the specific victim being targeted by a phishing scheme is the head or other high-profile member of an organization, it is referred to as whaling. Whereas general phishing attacks that are mass distributed to numerous potential victims do take efforts to make their fraudulent communications seem authentic, spear phishing and whaling attacks generally may be more detailed, the details of the communications being tailored to the specific target (Gil, 2018).

Phishing remains a popular method of attack for cybercriminals. As technology advances, cybersecurity has improved, making it more difficult for cybercriminals to find and exploit software weaknesses in computer networks. Although phishing attacks rely on human error instead of software weakness, it is still a viable way—and perhaps a more effective way—for a cybercriminal to infiltrate a computer network (Vanian, 2019).

Research suggests that most people do not fall prey to phishing attacks. In fact, one report found that 78 percent of people never click on phishing e-mails (Verizon, 2018). This does not mean, however, that phishing attacks are unsuccessful. That same report found that in a phishing attack, roughly 4 percent of the people who receive a phishing e-mail do click on them.

There are steps that can be taken to mitigate the harm of a phishing attack. Many phishing e-mails are kept from inboxes via a spam filter. Cybercriminals may devise ways to prevent their phishing e-mails from getting filtered, and thus relying solely on a spam filter may be insufficient to avoid a phishing attack. Because phishing e-mails can still sneak through, knowing how to identify a phishing e-mail is important. If the e-mail comes from someone unknown to the victim or from an organization with whom the victim does not conduct business, it is possibly a phishing attack and should not be opened or responded to (Federal Trade Commission, 2019). If a phishing e-mail is detected, reporting the e-mail can potentially help prevent harm to others from that phishing attack. In an organization, if one employee is hit by a phishing attack, it is possible that other employees were hit by the same attack. The sooner the attack is reported, the sooner the organization's cybersecurity personnel can respond to that attack and mitigate the damage done by it (Verizon, 2018). In addition to reporting a phishing attack to the appropriate people within an organization, phishing attacks—whether they be directed at members of an organization or at individuals in their personal capacity—can report the attack to governmental agencies, such as the Federal Trade Commission in the United States. Despite the benefits of reporting phishing attacks, it does not appear many people who detect a phishing attack ultimately report it. One report found that only 17 percent of phishing attacks are reported (Verizon, 2018).

See also: Financial Crimes; Personally Identifying Information; Social Engineering; Spam

Further Reading

Federal Trade Commission. 2019. "How to recognize and avoid phishing scams." https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Gil, Paul. 2018. "What is 'whaling?'" Lifewire, December 18, 2018. https://www.lifewire.com/what-is-whaling-2483605

Vanian, Jonathan. 2019. "Welcome to the next generation of corporate phishing scams." *Fortune*, June 19, 2019. http://fortune.com/2019/06/19/corporate-phishing-scams/

Verizon. 2018. "2018 data breach investigations report." 11th Edition. Verizon. https://www.phishingbox.com/assets/files/images/Verizon-Data-Breach-Investigations-Report-2018.pdf

PHREAKER

A phreaker is someone who hacks into telephone networks. Phreaking began to emerge in the 1950s when phreakers were able to hack into telephone networks through the use of specific tonal frequencies. By hacking into a telephone network, a phreaker could avoid paying for phone calls—even long distance ones. During the 1950s and 1960s, AT&T published articles in their technical journal regarding the use of frequencies to operate their telephone network, and even published some of the frequencies used (Breen and Dahlbom, 1960; Rosenbaum, 1971). This information aided phreakers in decoding the telephone system and devising ways to hack it.

Early on, phreaking involved discovering ways to replicate the necessary tonal frequencies to trick the telephone network into doing what a phreaker wanted it to do. Various ways of doing this were discovered. Joe Engressia—one of the first phreakers—discovered he was able to hack into the telephone network by whistling. Engressia was blind and had perfect pitch. While in college in 1968, Engressia was nearly kicked out of school for whistling to get classmates free phone calls (Terdiman, 2013). John Draper, another famous phreaker, discovered a way to replicate one specific tonal frequency—2,600 cycles per second—that enabled phreakers to make free long distance calls. He was able to replicate this tonal frequency using the toy whistle that came in boxes of Cap'n Crunch cereal. Accordingly, Draper donned the nickname Captain Crunch (Rosenbaum, 1971). One of the common ways devised to replicate the necessary tonal frequencies was the use of a blue box. A blue box is a machine designed to replicate the necessary tonal frequencies to hack a telephone network. Blue boxes could be purchased by a phreaker from fellow phreakers. For example, Steve Jobs and Steve Wozniak—the founders of Apple—created and sold blue boxes back in the 1970s, going by the phreaker handles Oaf Tobar and Berkeley Blue, respectively (Lapsley, 2013). Phreakers could also construct their own blue boxes if they were inclined. At least one publication in the 1970s (see Whipple, 1975) included instructions for constructing a blue box.

There can be disagreement as to whether phreaking is a "dead art" or whether it has simply evolved (Baraniuk, 2013). The use of blue boxes and similar methods to hack telephone networks is generally not used any more as cellular telephones have become prevalent. While the original methods of phreaking may not generally be used any more, hacking of telephone networks does still occur. In 2017, Muhammad Sohail Qasmani was sentenced to four years in prison for his conspiracy to commit wire fraud. Qasmani and his coconspirator, Noor Aziz Uddin (who is a still a fugitive as of early 2019), hacked the telephone networks of several United States businesses between 2008 and 2012. Several pay-per-minute phone lines were created by the pair, and phones from the hacked businesses called into those lines, incurring fees. The pair was ultimately able to steal nearly $20 million through this scheme (Federal Bureau of Investigation, 2017). The line between computers and telephones can blur at times. This can be seen with cellular telephones—devices that are clearly telephones, but also have the ability to perform the functions of a computer. Thus, determining whether the infiltration of a computer, network, or other device is phreaking or computer hacking may depend on what definitions of those activities someone subscribes to (see Baraniuk, 2013). The term "phracker" has been coined to describe someone who uses both phreaking and computer hacking to infiltrate a network.

See also: Draper, John; Engressia, Josef Carl, Jr.; Hacker and Hacking

Further Reading

Baraniuk, Chris. 2013. "Whatever happened to the phone phreaks?" *The Atlantic*, February 20, 2013. https://www.theatlantic.com/technology/archive/2013/02/whatever-happened-to-the-phone-phreaks/273332/

Breen, C., and C. A. Dahlbom. 1960. "Signaling systems for control of telephone switching." *The Bell System Technical Journal* 39, 6: 1381–1444.

Federal Bureau of Investigation. 2017. "Dialing for cash: Pakistani man sentenced for laundering millions in Telecom hacking scheme." July 6, 2017. https://www.fbi.gov/news/stories/telecom-hacking-scheme

Lapsley, Phil. 2013. "The definitive story of Steve Wozniak, Steve Jobs, and phone phreaking." *The Atlantic*, February 20, 2013. https://www.theatlantic.com/technology/archive/2013/02/the-definitive-story-of-steve-wozniak-steve-jobs-and-phone-phreaking/273331/

Rosenbaum, Ron. 1971. "Secrets of the little blue box." *Esquire*, October 1, 1971. https://classic.esquire.com/article/1971/10/1/secrets-of-the-blue-box

Terdiman, Daniel. 2013. "Unlocking Ma Bell: How phone phreaks came to be." *CNet*, February 12, 2013. https://www.cnet.com/news/unlocking-ma-bell-how-phone-phreaks-came-to-be/

Whipple, Spencer, Jr. 1975. "Inside Ma Bell." *73 Magazine* (June): 67–80. https://archive.org/details/73-magazine-1975-06/page/n67

PIGGYBACKING

Piggybacking is a method that can be used by cybercriminals to gain unauthorized access to a restricted area. Those restricted areas can be digital areas, such as a computer network, or they can be physical areas, such as a computer lab. With either type of location, the method of gaining unauthorized access is the same. The cybercriminal trails someone who has made legitimate entry to the restricted area and enters along with them (Parker, 1989).

Digital piggybacking can take place in a couple ways. One method cybercriminals might employ is using a computer that is already logged into a computer network. Something like this could occur if a user uses a public computer (e.g., at the library) and does not log out of an account (e.g., e-mail account, bank account, social media account) before leaving that public computer. A cybercriminal can use that computer to gain access to the previous user's accounts, which enables a cybercriminal to potentially obtain personally identifying information of that previous user. That information can in turn be used to commit identity theft or various financial crimes.

Another method of digital piggybacking is the use of unsecured Wi-Fi networks. Cybercriminals can do this using an electronic device that has the ability to connect to a Wi-Fi network, and then checking to see if the network is password protected. If it is not, the cybercriminal will be able to access the network. There are those who engage in wardriving—driving around and identifying the unsecured Wi-Fi networks in a given area. A log of unsecured Wi-Fi connections may be made available online by a wardriver. A wardriver might also leave chalk markings near an unsecured Wi-Fi location—a practice known as warchalking (Berghel, 2004). Those who access an unsecured Wi-Fi network may do so for several reasons. They may do so simply to access the internet without having to pay for internet service themselves. If the Wi-Fi network is not provided as a free-to-the-public network, this can be a form of utility theft. This is so even though the entity hosting the network would not necessarily be deprived of anything by having another party piggyback on the network. There are other reasons a person might access an unsecured Wi-Fi network that can be detrimental to the entity hosting it. It is possible for cybercriminals to access other electronic devices connected to a Wi-Fi network. If there is personally identifying information on those devices, the cybercriminal could steal that information. It is possible a cybercriminal might also use an unsecured Wi-Fi network to commit other cybercrimes online (McAfee, 2014). By using someone else's network to commit a cybercrime, a cybercriminal can make it more difficult for law enforcement to trace the criminal actions back to them.

Physical piggybacking can also be used to commit cybercrime. Physical piggybacking occurs when someone follows a person that is authorized to access a physical area through a security checkpoint. This can happen if an employee of a business uses an electronic key card to get in the front door of the business, and another person following behind them enters at the same time. By having access to restricted areas, a cybercriminal can potentially access sensitive information. A cybercriminal might combine physical piggybacking with digital piggybacking.

Once they gain access to a restricted physical area, they might be able to log on to a computer within that area that an employee has logged into for the day.

Piggybacking is something that individuals can take steps to protect against. For digital piggybacking, taking the time to verify you have logged off a computer when you are away from it—be that a public computer, a computer at your place of employment, and so forth—can help prevent someone from piggybacking. For Wi-Fi networks, ensuring a password is in place can help prevent piggybacking. Turning the Wi-Fi network off when it is not in use can also help (McAfee, 2014). For physical piggybacking, prohibiting people you do not know from following you into restricted areas can cut off potential piggybacking attempts.

See also: Financial Crimes; Identity Theft; Password; Personally Identifying Information; Wardriving

Further Reading

Berghel, Hal. 2004. "Wireless infidelity I: War driving." *Communications of the ACM* 47, 9: 21–26.

McAfee. 2014. "What is wardriving?" McAfee, June 23, 2014. https://securingtomorrow.mcafee.com/consumer/identity-protection/wardriving/

Parker, Donn B. 1989. "Computer crime: Criminal justice resource manual." United States Department of Justice. https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf

PILE, CHRISTOPHER (1969–)

Christopher Pile is a creator of viruses and other malware from the United Kingdom. In 1994, Pile was arrested by law enforcement for the malware he released. He released the malware under the online name of Black Barron (Victor, 1995). He pleaded guilty to all charges against him in 1995. He became the first person in the United Kingdom to receive a sentence of incarceration for creating computer viruses (Bates, 2015).

There were three primary pieces of malware that Pile released. The names of these pieces of malware were all named after terms used in the British television show Red Dwarf (Victor, 1995). He wrote two viruses, named Pathogen and Queeg. Perhaps the most impactful piece of malware Pile wrote was SMEG (Simulated Metamorphic Encryption Generator). SMEG was a piece of malware that could be attached to other viruses. Once attached, SMEG would randomize the code of the virus, creating up to four million different permutations of the virus. Pile's other two viruses were amplified using SMEG (Delio, 2002; Victor, 1995). The viruses would attach to the files of an infected computer and cause them to expand. This happened until all the memory on the computer was filled, rendering the computer inoperable (Victor, 1995). Pile hid the viruses in software—computer games and in at least one instance, a piece of antivirus software—and made the software available through electronic bulletin boards where victims would download them (Victor, 1995).

At the time of Pile's arrest, law enforcement executed a search warrant at his residence. A computer located during the search was found to have been wiped clean. Investigators were able to ultimately recover some data from the computer, namely two job applications with Pile's name on them. Investigators also found encrypted data on floppy disks from Pile's residence. Pile initially denied involvement with the malware he had created. However, once investigators confronted Pile with the fact they had found the encrypted file on floppy disks, he admitted his involvement and provided the investigators with the password for the encrypted file. The file was the source code for several viruses (Bates, 2015). When asked by investigators why he had created the viruses, Pile claimed he did it because—at the time—there were not many viruses available from U.K. writers, and that writing the viruses raised his self-esteem (Victor, 1995).

Several people had been impacted by Pile's viruses. Several victims came forward and provided evidence to law enforcement that their computers had been impacted. Some victims came forward but later denied they had been impacted. It appears these denials were made by some companies that had been victimized, looking to keep quite the fact they had been impacted (Bates, 2015). It is estimated that Pile's viruses caused over $1 million in damage (Victor, 1995). Pile was charged with 11 counts: 10 counts of distributing malware and one count of incitement for distributing SMEG. He was sentenced to six months of prison on the first 10 counts, all of which ran concurrently. On the incitement charge, he was sentenced to 12 months of prison to run consecutive to the six months of prison on the other 10 charges. This totaled an 18-month prison sentence (Bates, 2015).

See also: Malware; Motives; Virus

Further Reading

Bates, Jim. 2015 (1996). "Throwback Thursday: Regina v Christopher Pile: The inside story." *Virus Bulletin*. https://www.virusbulletin.com/virusbulletin/2015/04/throwback-thursday-regina-v-christopher-pile-inside-story-february-1996

Delio, Michelle. 2002. "A virus writer heads to prison." *Wired*, May 3, 2002. https://www.wired.com/2002/05/a-virus-writer-heads-to-prison/

Victor, Peter. 1995. "'Black Baron' a self-taught whiz-kid." *The Independent*, November 16, 1995. https://www.independent.co.uk/news/black-baron-a-self-taught-whiz-kid-1582109.html

PLANKTON

Plankton is malware that was discovered in 2011 by Xuxian Jiang, a professor of computer science at North Caroline State University. The malware is designed for devices running the Android operating system. The malware functions as both a Trojan horse and spyware (Jiang, 2011; Microsoft, 2011).

Plankton was spread through the downloading of applications that marketed themselves as legitimate but had the Plankton malware contained within. Several applications containing Plankton were available on the Official Android Market (now known as Google Play) for two months prior to the malware being discovered, and some of those applications had been downloaded over 100,000 times (Jiang, 2011; Svajcer, 2011). Once one of those applications was downloaded, Plankton would run a service in the background that would collect data from the infected device and send it to a server presumably controlled by the designers of the malware. The malware was able to access data that the underlying application was given permission to access (Shipman, 2011). The data Plankton was capable of collecting included internet browsing history, device activity, device location, and user ID (Microsoft, 2011; Shipman, 2011). The malware also contained code that could permit it to retrieve login credentials (username and password) for accounts of the device's user, such as social media accounts and e-mail accounts. However, at the time of its discovery, there was no indication that this functionality had been utilized yet (Goodin, 2011; Jiang, 2011).

In addition to its spyware capabilities, Plankton also functioned as a Trojan horse. It permitted malware to be downloaded to the infected device from a remote server. The initial payload downloaded was the spyware noted above. However, Plankton was designed to permit the download of additional malware on infected devices in the future (Jiang, 2011; Shipman, 2011).

The design of Plankton is what allowed it to avoid detection for several months. The method employed by Plankton was a method that Google had been made aware of roughly a year prior to the discovery of Plankton. Jon Oberheide—a computer security expert—discovered an exploit in Google's system. Namely, Google's application market had a function that permitted Google to remotely install application data on a user's device. Oberheide warned that if a cybercriminal were able to spoof the commands trying to install data, they could download malware to users' devices (Metz, 2010; Oberheide, 2010). Jiang noted that Plankton appears to have used the exploit discovered by Oberheide (Jiang, 2011). Following the discovery of Plankton, some criticized Google for not implementing more robust security measures in its application marketplace. At the time, Google had not implemented a system of code signing—a system where Google would have had to verify the legitimacy of code distributed through its marketplace (Goodin, 2011; Svajcer, 2011). Apple had implemented such procedures at the time, and Plankton did not affect its operating systems (Goodin, 2011).

See also: Exploit Kit; Password; Payload; Spoofing; Spyware; Trojan Horse

Further Reading

Goodin, Dan. 2011. "Toxic Plankton feeds on android market for two months." *The Register*, June 13, 2011. https://www.theregister.co.uk/2011/06/13/android_market_still_insecure/

Jiang, Xuxian. 2011. "Security alert: New stealthy android spyware—Plankton—Found in Official Android Market." North Carolina State University. https://www.csc2.ncsu.edu/faculty/xjiang4/Plankton/

Metz, Cade. 2010. "Google can kill or install apps on citizen Androids." *The Register*, June 28, 2010. https://www.theregister.co.uk/2010/06/28/google_remote_android_application_install/

Microsoft. 2011. "Trojan:AndroidOS/Plankton.A." Microsoft. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan%3AAndroidOS%2FPlankton.A

Oberheide, Jon. 2010. "Remote kill and install on Google Android." Jon Oberheide (blog), June 25, 2010. https://jon.oberheide.org/blog/2010/06/25/remote-kill-and-install-on-google-android/

Shipman, Matt. 2011. "More bad news: Two new pieces of Android Malware—Plankton and YZHCSMS." North Carolina State University, June 9, 2011. https://www.youtube.com/watch?v=ZD_QjAlyrow&list=PLR9aD4y1pbrxNT2lxpehWa_tDsoyFr9lY&index=8

Svajcer, Vanja. 2011. "Plankton malware drifts into Android Market." Sophos, June 14, 2011. https://nakedsecurity.sophos.com/2011/06/14/plankton-malware-drifts-into-android-market/

POKÉMON GO

Pokémon Go is a mobile augmented reality game that was released on July 6, 2016, in the United States, and it has been released in other countries as well. The game has players travel to physical locations to capture virtual creatures known as Pokémon. The game uses global positioning system (GPS) to determine the physical location of players. This, in turn, allows the game to know whether a player is close to a Pokémon or other key location in the game. There have been several incidents where criminals waited at key physical locations to commit crimes against players who went to those locations.

Pokémon Go has been involved with several criminal incidents since its inception. In its first couple of month in the United Kingdom, there were 290 police incidents reported that involved *Pokémon Go* (Criddle, 2016). Within the first week of its release, *Pokémon Go* was being used as a tool to commit crime. Four teenagers in Missouri were using a feature of the game called a beacon. A beacon is designed to lure Pokémon. Because a beacon lures Pokémon, it also attracts players to the location looking to catch Pokémon. It initially appeared that the teens set up these beacons and waited for players to show up, at which point they would rob them (Garber-Paul, 2016). However, law enforcement ultimately determined that the teenagers simply waited at hotspots already in place in the game to find their victims (Hollinshed and Byers, 2016). It also appears that not all of the robberies committed by the teenagers were aided by their use of *Pokémon Go* (Currier, 2017). Three of the teenagers were charged with robbery and the fourth was placed in the custody of the juvenile system (Hollinshed and Byers, 2016).

Just days after these robberies in Missouri, another person committed several robberies on the University of Maryland campus that appear to have used *Pokémon Go* to accomplish them. Several of the victims were playing *Pokémon Go* when their mobile phones were stolen from them (Hedgpeth, 2016). Similar crimes occurred outside the United States as well. In Manchester, United Kingdom, beacons were used by robbers to lure in victims (Criddle, 2016). It is not just *Pokémon Go*'s GPS interactivity that enables criminals to target victims. Those distracted by the game in general by looking down at their mobile phone screen also appear to have been targeted. Shortly after the release of *Pokémon Go* in the United Kingdom, a number of citizens in Southwark had their mobile phones stolen from them by people on mopeds. Those criminals would target people who were looking at their phones—whether they were playing *Pokémon Go* or engaging in other activity on their mobile phone (Southwark News, 2016).

Based on these early uses of *Pokémon Go* to lure in victims, there was concern that the game might be used for more nefarious purposes, such as pedophiles luring children to their location (Criddle, 2016; Garber-Paul, 2016). These concerns were heightened when a report discovered that the developers of *Pokémon Go* unintentionally placed Pokémon at locations in New York city that were in front of the residences of registered sex offenders. There was some indication that a similar thing was occurring in other states, such as California (Baitinger and Musumeci, 2016). The state of New York went so far as to ban convicted sex offenders from playing *Pokémon Go* or similar games as a term of their parole (Vasquez, 2016). There have been some incidents involving *Pokémon Go*, sex offenders, and children. In two separate incidents—one in Indiana and the other in Wales—sex offenders were found playing *Pokémon Go* with minors just outside of courthouses (BBC News, 2016; Vasquez, 2016). A separate incident in Wales involved a man who invited children to his home on the premise that numerous Pokémon were present there, though it is not clear whether the man was a sex offender or what his intentions were (Criddle, 2016).

In addition to the physical threats posed to those who play *Pokémon Go*, there are cyber threats as well. Fraudulent versions of *Pokémon Go* were apparently designed when the game was released. These versions would download malware to the victim's phone, which could result in the theft of information contained on that phone (Criddle, 2016).

While players of *Pokémon Go* face the risk of being the victims of one of the crimes described above, they could also be involved in crimes arising from their use of the game. One concern is drivers being distracted by *Pokémon Go*, resulting in car accidents. These incidents may go beyond mere distracted driving. Drivers might intentionally drive in illegal ways in order to catch Pokémon while driving. The game is only designed to operate if the mobile phone is traveling under 20 miles per hour. This results in people driving slowly in locations that require a higher speeds and in people abruptly stopping to catch a Pokémon once it is found (Criddle, 2016; Garber-Paul, 2016). Players might also exploit the game to catch Pokémon in a manner not permitted by the game. Specifically, players can spoof the GPS coordinates of their mobile phone in order to catch Pokémon without ever leaving their homes (Malwarebytes, 2019). Users doing this would violate the game's terms of service (Niantic, 2019). Spoofing GPS coordinates could allow players to access in-game content—such as usable items in the game—in a more expeditious fashion than would be physically possible without GPS spoofing. Where this allows players to avoid purchasing items in the game, it could be viewed as theft.

See also: Malware; Spoofing

Further Reading

Baitinger, Brooke, and Natalie Musumeci. 2016. "Pokémon Go lures children near homes of sex offenders." *New York Post*, July 29, 2016. https://nypost.com/2016/07/29/pokemon-go-lures-children-near-homes-of-sex-offenders/

BBC News. 2016. "Pokemon Go: Sex offender caught playing game with child." *BBC News*, July 15, 2016. https://www.bbc.com/news/technology-36804245

Criddle, Cristina. 2016. "Robberies, thefts, assaults and driving offences among hundreds of crimes involving Pokemon Go logged by police in July." *The Telegraph*, August 29, 2016. https://www.telegraph.co.uk/news/2016/08/29/robberies-thefts-assaults-and-driving-offences-among-hundreds-of/

Currier, Joel. 2017. "Alleged 'Pokemon Go' robbers are charged in St. Louis crime spree." *St. Louis Post-Dispatch*, April 28, 2017. https://www.stltoday.com/news/local/crime-and-courts/alleged-pokemon-go-robbers-are-charged-in-st-louis-crime/article_11f52da9-c124-566e-b5a1-cd765be58d92.html

Garber-Paul, Elisabeth. 2016. "Is 'Pokemon Go' really driving a crime wave?" *Rolling Stones*, July 12, 2016. https://www.rollingstone.com/culture/culture-news/is-pokemon-go-really-driving-a-crime-wave-163215/

Hedgpeth, Dana. 2016. "Police look for suspect wanted in Pokémon Go thefts at U-Md." *Washington Post*, July 19, 2016. https://www.washingtonpost.com/local/public-safety/police-look-for-suspect-wanted-in-pokemon-go-thefts-at-u-md/2016/07/19/0ab9aa98-4dd2-11e6-a422-83ab49ed5e6a_story.html?utm_term=.c90ead293ec0

Hollinshed, Denise, and Christine Byers. 2016. "Robbers target players of popular 'Pokemon Go' smartphone game, police in O'Fallon, Mo., say." *St. Louis Post-Dispatch*, July 11, 2016. https://www.stltoday.com/news/local/crime-and-courts/robbers-target-players-of-popular-pokemon-go-smartphone-game-police/article_ca161f27-37b7-57bb-bfa6-a30b0563e3f0.html

Malwarebytes. 2019. "Spoofing." Malwarebytes. https://www.malwarebytes.com/spoofing/

Niantic. 2019. "Niantic terms of service." https://nianticlabs.com/terms/en/

Southwark News. 2016. "Pokemon Go and mopeds thefts: Police urge caution as people take to the streets with their phones on display." *Southwark News*, July 15, 2016. https://www.southwarknews.co.uk/news/pokemon-go-mopeds-thefts-police-urge-caution-people-take-streets-phones-display/

Vasquez, Justina. 2016. "New York Bans Registered Sex Offenders From Pokémon Go." National Public Radio, August 2, 2016. https://www.npr.org/sections/alltechconsidered/2016/08/02/488435018/new-york-bans-registered-sex-offenders-from-pok-mon-go

POLITICAL USES

Cybercrime can be used to advance political purposes. Cybercriminals who commit cybercrimes for this purpose can be divided into two general categories: those whose actions are sanctioned—either explicitly or tacitly—by the government of the country they live in and those who whose actions are not so sanctioned.

Those who commit cybercrimes that are sanctioned by their government generally do not view their activities as illegal. Inasmuch as their government is permitting their activities, those activities at least appear to be in conformity with the laws of the country they live in (Ablon, 2018). In some instances, those engaging in cyberattacks are employed by their government, and the government is directing the attacks. This can be seen with the People's Liberation Army (PLA) Unit 61398 in China. The PLA is the Chinese military and thus is under the control of the Chinese government. Unit 61398 is designed to carry out cyberespionage against foreign businesses. The businesses targeted by Unit 61398 are in industries that China has identified as strategically important for its economic growth. Espionage efforts by Unit 61398 have allowed China to steal technological intellectual property and business information from these foreign businesses (Mandiant, 2013). While the country from which the cyberattack originated may not view the actions as illegal, the countries that house the victimized businesses would. This can be so even when the country that is attacked carries out similar attacks on other countries. For example, several companies in the United States have been the victim of espionage efforts by the PLA, and in 2014, the United States has indicted members of the PLA involved in those cyberattacks (United States Department of Justice, 2014). The United States, in conjunction with Israel, is believed to have used the Stuxnet computer worm to attack Iran's Natanz nuclear facility in 2010. The attack caused computers at the facility to spin centrifuges rapidly, to the point the centrifuges were damaged (Warrick, 2011). The attack has not been treated as a criminal matter in the United States.

Some cybercriminals are not directly employed by the government of the country in which they live, but their activities are tacitly approved of by the government. The Syrian Electronic Army is an example of this. It has carried out attacks on the websites and social media accounts of entities opposed to the Syrian government and entities in Western countries (Helmi, 2019). The Syrian Electronic Army does not appear to work for the Syrian government. However, Bashar al-Assad—president of Syria—has voiced appreciation for the efforts of the group (Fowler, 2013; Helmi, 2019). Thus, it has not faced criminal repercussions in Syria. A similar organization is the Internet Research Agency (IRA) in Russia. The IRA created false social media accounts that were used to influence the electorate in the United States leading up to the 2016 presidential election. The IRA is not part of the Russian government, but it appears to have ties to Russia president Vladimir Putin and appears to share the same goals as the Russian government; leading up to the 2016 presidential election, Russia's Main Intelligence Directorate of the General Staff (GRU) was engaged in efforts to influence the election as well. Specifically, the GRU was infiltrating the computer networks of individuals and other entities associated with presidential candidate Hilary Clinton (Mueller, 2019). While the IRA was indicted in the United States, there have been no criminal repercussions in Russia.

Other groups have a political agenda they pursue through their cybercrime, but they are not sponsored by the government of the country in which they live. Accordingly, their actions are not likely to be viewed as legal. An example of a political hacking group that is not state-sponsored would be Ghost Squad. The group conducted DDoS attacks against the websites of the Ku Klux Klan and the Black Lives Matter movement in 2016. The attack against the Ku Klux Klan was motivated by Ghost Squad's opposition to the racist goals of the Ku Klux Klan (Chang, 2016). The attack against the Black Lives Matter movement was similarly motivated, as Ghost Squad believed the actions of some in the movement were equally as racist as those of members of the Ku Klux Klan (Russon, 2016).

See also: Distributed Denial-of-Service Attack (DDoS); Hacktivism; International Issues; Motives; People's Liberation Army Unit 61398; Russia; Operation Olympic Games; Syrian Electronic Army; U.S. Presidential Election Interference, 2016

Further Reading

Ablon, Lillian. 2018. “Data thieves: The motivations of cyber threat actors and their use and monetization of stolen data.” Rand Corporation, March 15, 2018. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf

Chang, Lulu. 2016. “Hackers attack KKK and briefly bring down main website.” Fox News, April 25, 2016. https://www.foxnews.com/tech/hackers-attack-kkk-and-briefly-bring-down-main-website

Fowler, Sarah. 2013. “Who is the Syrian Electronic Army?” BBC, April 25, 2013. https://www.bbc.com/news/world-middle-east-22287326

Helmi, Norman. 2019. “The Emergence of open and organized pro-government cyber attacks in the Middle East: The case of the Syrian Electronic Army.” OpenNet Initiative. https://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army

Mandiant. 2013. “APT1: Exposing one of China’s cyber espionage units.” Mandiant. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Mueller, Robert S. 2019. “Report on the investigation into Russian interference in the 2016 presidential election.” Volume 1. United States Department of Justice. https://www.justice.gov/storage/report.pdf

Russon, Mary-Ann. 2016. “Anonymous takes down Black Lives Matter website to make point that ‘All Lives Matter.’” *International Business Times*, May 4, 2016. https://www.ibtimes.co.uk/anonymous-takes-down-black-lives-matter-website-make-point-that-all-lives-matter-1558004

United States Department of Justice. 2014. “U.S. charges five Chinese military hackers for cyber espionage against U.S. corporations and a labor organization for commercial advantage.” May 19, 2014. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

Warrick, Joby. 2011. “Iran’s Natanz nuclear facility recovered quickly from Stuxnet cyberattack.” *Washington Post*, February 16, 2011. http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html

POULSEN, KEVIN (1965–)

Kevin Lee Poulsen, also known as Dark Dante, is a former black-hat hacker whose interest in computers began when he was young. Poulsen is probably best known for taking over all of the phone lines of KIIS-FM in 1990, a radio station in Los Angeles, so that he would be the 102nd caller and win a Porsche 944 S2. He eventually won another car, two vacation trips to Hawaii, and cash winnings of $50,000, but he faced criminal charges resulting from the events.

Poulsen was born on November 30, 1965, in Pasadena, California. When he was 17, Poulsen hacked into the U.S. Department of Defense’s Arpanet, the computer network created by the Pentagon that eventually became today’s internet. He was never charged with any criminal activity for this. From there he accessed the University of California Berkeley’s computers and accessed military research being carried out there. He was not prosecuted for that behavior because he was a minor. Instead, he was given a warning.

Poulsen rented a storage locker but failed to make the payments on it, so in February 1988, the locker was opened. Officials found computer and telephone equipment along with the phone number for the Soviet embassy. From this, law enforcement assumed that the owner of the locker was working with the Soviet Union as a spy. Upon finding many items with the name "Kevin Poulsen," agents searched his home. There they found a wiretapping operation that allowed Poulsen to monitor others' telephone conversations.

The FBI began a national search for Poulsen, who chose to run from agents and become a fugitive from the law. During this time he was highlighted on the TV show *Unsolved Mysteries*. Oddly, the call-in hotlines for the show crashed after his picture appeared on the screen. He was arrested in April of 1991 after 18 months in hiding. Employees at a grocery store recognized Poulsen and tackled him and then waited for law enforcement to arrive. Poulsen was held without bail for five years, then pleaded guilty to computer fraud, money laundering, and obstruction of justice.

The sentencing judge ordered Poulsen to refrain from using computers. In order to remain active in the computer industry, he became a journalist. He accepted a position at *SecurityFocus* as the editorial director, where he investigated computer hacking. Some of the stories he contributed included one about a hospital where patient records were released, an Ohio power plant where a computer virus had attacked the safety system, the value of Apple's encryption of personal data on iPhones, and a hacker from Ukraine who helped the FBI with computer security. A few years later, Poulsen became a contributing editor at *Wired*, a technical journal. He is also a contributor for the *Daily Beast*. He has assisted law enforcement personnel who were investigating sexual predators on Myspace. He was able to help identify over 700 registered sex offenders who had profiles on the site. In June 2010, Poulsen reported the story of the arrest of Chelsea Manning. He also served as the advisor on hacking activities for the movie *Blackhat*.

Along with Aaron Swartz and James Dolan, Polusen created SecureDrop (formerly called DeadDrop), a software system that allows for a secure method of communication between journalists and their sources who possess sensitive information or documents. The program is now overseen by the Freedom of the Press Foundation. Poulsen is a member of their technical advisory board. He also became a programmer at SRI International and Sun Microsystems, and was hired by the Pentagon's security branch to serve as a consultant to test their computer security.

See also: Advanced Research Projects Agency Network; Black-Hat Hackers; DEF CON; Hacker and Hacking; Mitnick, Kevin; Swartz, Aaron

Further Reading

Littman, Jonathan. 1997. *The watchman: The twisted life and crimes of serial hacker Kevin Poulsen*. Boston, MA: Little, Brown and Company.

Poulsen, Kevin. 2011. *Kingpin: how one hacker took over the billion-dollar cybercrime underground*. New York: Crown Publishers.

Poulsen, Kevin. 2015. "Surprise! America already has a Manhattan project for developing cyber attacks." *Wired*, February 18, 2015. https://www.wired.com/2015/02/americas-cyber-espionage-project-isnt-defense-waging-war/

Poulsen, Kevin. 2016. "The future of security: The bottom line." *Wired*, February 12, 2016. https://www.wired.com/2016/02/the-future-of-security-the-bottom-line/

PRESIDENT AND CYBERCRIME

Presidential statements and actions on cybercrime can have an impact on the laws and policies that regulate online activities throughout the United States and the world. Since cybercrime is a relatively new activity, there have been only four presidents who have spoken about online crimes and their plans to thwart such activity.

Democrat Bill Clinton was the first president to mention the problem of cybercrime. In 1996, during his first term in office, Clinton established the first Commission on Critical Infrastructure that had the responsibility to identify the nation's critical infrastructures that were at risk of either a physical attack or a cyberattack. In doing so, he was specifically concerned with those infrastructures that rely on computer systems to operate, which would make them more of a target to hackers. Clinton described the need for such a strategy in a speech he gave in 2000. He indicated that the country's critical systems, including the power structures, nuclear plants, air traffic control, and computer networks, are all connected by computers. He described one incident in which a satellite malfunctioned, disrupting technology around the world. To help protect against cyberevents like these, Clinton worked with members of both the public and the private sectors to develop a national plan to increase the nation's cybersecurity (Clinton, 2000).

Clinton also provided money for counterterrorism and cybercrime programs carried out by the Department of Justice. In an Appropriations Act in 2001, Clinton provided $100 million that would help fund "State and local first-responder training, staff support for the Joint Terrorism Task Forces and enhanced technology and intelligence-gathering along the northern border" (Clinton, 2001).

In the days after the terrorist attacks of September 11, 2001, Republican President George W. Bush established a committee that would create a strategy to improve the country's cybersecurity. He appointed Richard Clarke to serve as the National Cybersecurity Advisor, and gave him the task of reviewing vulnerabilities that existed in cyberspace. Another task given to Clarke was to review the tactics that terrorist groups use to recruit people who have advanced cyber skills.

Bush initiated several approaches to fighting cybercrime. One was to work cooperatively with the leaders of other nations to address the problem. For example, in 2001, Bush described his interaction with the European Union regarding cybercrime, "We emphasize the need to take mutually reinforcing action in response to common problems in fighting international crime. We have, therefore, launched multi-annual cooperation in several areas, such as . . . cybercrime" (Bush, 2001). He also issued a statement after meeting with the prime minister of India, Manmohan Singh, in which he said the two countries "recognized the importance of capacity building in cyber security and greater cooperation to secure their growing electronic interdependencies, including to protect electronic transactions and critical infrastructure from cybercrime, terrorism and other malicious threats" (Bush, 2006).

Another approach Bush took toward combating cybercrime was to support the Council of Europe Convention on Cybercrime. In asking for the Senate to ratify the document, Bush said that the convention would help combat global cybercrime "By providing for broad international cooperation in the form of extradition and mutual legal assistance, the Cybercrime Convention would remove or minimize legal obstacles to international cooperation that delay or endanger U.S. investigations and prosecutions of computer-related crime" (Bush, 2003). As a result, Bush said the convention would deny "safe havens" to terrorists and other cybercriminals. The U.S. Senate ratified it on August 3, 2006, and President Bush signed it on September 22, 2006. The convention became effective for the United States on January 1, 2007.

In 2013, Democratic President Barack Obama called cybercrime "one of the most serious economic national security challenges that we face as a nation." Although Obama understood that the internet provides "incredible information and allows us to reach out around the world also makes our bank accounts vulnerable," he also realized that cybercrime "is a huge problem and a growing problem. And so we've got to be in there in some way to help protect the American people, even as we're also making sure that government doesn't abuse it" (Obama, 2013a).

Recognizing that cybercrime did not affect only one country, Obama sought international cooperation. After meeting with the leader of the United Kingdom, David Cameron, Obama said, "We believe we can make (our) relationship even stronger with deeper cooperation in areas critical to . . . our national security, like cybercrime" (Obama, 2011b). After speaking with leaders from North America, including Canadian Prime Minister Stephen Harper and Mexican President Felipe de Jesus Calderon Hinojosa, Obama reported that they "underscore that fighting cybercrime is essential to promoting economic growth and international security" (Obama, 2012).

Obama also talked to the leaders of Estonia, Latvia, and Lithuania about cybercrime. Afterward, he promised to strengthen the United States' attention to cybercrime, both regionally and around the world. He sought to work closely with members of both the public and private sectors and to cooperate with law enforcement agencies from other countries to investigate and prosecute acts of cybercrime. In the end, Obama described the goal of an open, secure, and reliable internet that promotes the free flow of information but at the same time protects the privacy of users (Obama, 2013b). Obama also spoke with the leaders of Japan, India, Brazil, China, Singapore, and Cuba about the need to increase cybersecurity. Finally, Obama sought to attack transnational criminal organizations "that engage in cybercrime, threaten sensitive public and private computer networks, undermine the integrity of the international financial system, and impose costs on the American consumer" (Obama, 2011a).

Upon beginning his term as president in 2017, Republican Donald Trump announced that it would be the policy of the executive branch to "strengthen enforcement of Federal law in order to thwart transnational criminal organizations . . . that are related to . . . cybercrime" (Trump, 2017a).

Like other presidents, Trump also took an international approach to fighting cybercrime. After meeting with the leaders of Malaysia, Trump said, "The United States and Malaysia acknowledged that cyber and other crimes often help finance terrorist networks. The countries committed to utilize available multilateral instruments . . . in order to strengthen domestic legislation and foster international cooperation in combating cybercrime" (Trump, 2017b). He followed that with a statement after meeting with leaders in the Asia-Pacific Economic Summit, saying we "must also deal decisively with other threats to our security and the future of our children, such as . . . cybercrime" (Trump, 2017d). Finally, Trump also spoke with the leaders from Vietnam and explained that "we continue to work with our Vietnamese partners and with partners across the region on a range of challenges, including . . . cybercrime" (Trump, 2017c).

See also: CAN-SPAM Act of 2003; Comprehensive National Cybersecurity Initiative; Computer Fraud and Abuse Act of 1986; Cybersecurity Act of 2012; Cybersecurity Enhancement Act of 2014; Cybersecurity Workforce Assessment Act of 2015; Digital Millennium Copyright Act; Federal Information Security Management Act of 2002; National Cybersecurity and Critical Infrastructure Protection Act of 2013; Personal Data Notification and Protection Act of 2017

Further Reading

Bush, George W. 2001. "Göteborg statement: Summit of the United States of America and the European Union." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, June 14, 2001. https://www.presidency.ucsb.edu/node/217077

Bush, George W. 2003. "Message to the Senate transmitting the Council of Europe Convention on Cybercrime." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, November 17, 2003. https://www.presidency.ucsb.edu/node/215821

Bush, George W. 2006. "Joint statement between the United States of America and India." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, March 2, 2006. https://www.presidency.ucsb.edu/node/214288

Clinton, William J. 2000. "Commencement address at the United States Coast Guard Academy in New London, Connecticut." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, May 17, 2000. https://www.presidency.ucsb.edu/node/227708

Clinton, William J. 2001. "Statement on signing the Departments of Commerce, Justice, State, the Judiciary, and Related Agencies Appropriations Act, 2001." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, December 21, 2001. https://www.presidency.ucsb.edu/node/228552

Obama, Barack. 2011a. "Message to the Congress reporting on the executive order blocking property of transnational criminal organizations." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, July 24, 2011. https://www.presidency.ucsb.edu/node/290734

Obama, Barack. 2011b. "The president's news conference with Prime Minister David Cameron of the United Kingdom in London." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, May 25, 2011. https://www.presidency.ucsb.edu/node/290330

Obama, Barack. 2012. "Joint statement by North American leaders." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, April 2, 2012. https://www.presidency.ucsb.edu/node/300810

Obama, Barack. 2013a. "Interview with Chris Matthews on MSNBC's 'Hardball' at American University." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, December 5, 2013. https://www.presidency.ucsb.edu/node/327088

Obama, Barack. 2013b. "Joint statement by President Barack Obama, President Toomas Hendrik Ilves of Estonia, President Andris Berzins of Latvia, and President Dalia Grybauskaite of Lithuania." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, August 30, 2013. https://www.presidency.ucsb.edu/node/304926

Obama, Barack. 2014. "Joint statement by President Obama and Prime Minister Shinzo Abe of Japan: The United States and Japan: Shaping the future of the Asia-Pacific and beyond." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, April 25, 2014. https://www.presidency.ucsb.edu/node/306024

Obama, Barack. 2015a. "Joint communique by President Obama and President Dilma Rousseff of Brazil." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, June 30, 2015. https://www.presidency.ucsb.edu/node/310913

Obama, Barack. 2015b. "Joint statement by President Obama and Prime Minister Narendra Modi of India—Shared effort, progress for all." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, January 25, 2015. https://www.presidency.ucsb.edu/node/309229

Obama, Barack. 2015c. "Remarks prior to a meeting with President Xi Jinping of China in Le Bourget, France." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, November 30, 2015. https://www.presidency.ucsb.edu/node/311603

Obama, Barack. 2016a. "Directive on United States–Cuba normalization." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, October 14, 2016. https://www.presidency.ucsb.edu/node/319096

Obama, Barack. 2016b. "Joint statement by President Obama and Prime Minister Lee Hsien Loong of Singapore." Online by Gerhard Peters and John T. Woolley, The American Presidency Project. https://www.presidency.ucsb.edu/node/319878

Trump, Donald J. 2017a. "Executive Order 13773—Enforcing Federal Law With Respect to Transnational Criminal Organizations and Preventing International Trafficking." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, February 9, 2017. https://www.presidency.ucsb.edu/node/32373

Trump, Donald J. 2017b. "Joint statement—Enhancing the comprehensive partnership between the United States of America and Malaysia." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, September 13, 2017. https://www.presidency.ucsb.edu/node/331106

Trump, Donald J. 2017c. "The president's news conference with President Tran Dai Quang of Vietnam in Hanoi, Vietnam." Online by Gerhard Peters and John T. Woolley, The American Presidency Project, November 12, 2017. https://www.presidency.ucsb.edu/node/331366

Trump, Donald J. 2017d. "Remarks at the Asia-Pacific Economic Cooperation CEO Summit in Danang, Vietnam." Online by Gerhard Peters and John T. Woolley, The American Presidency Project. https://www.presidency.ucsb.edu/node/331585

PRETTY GOOD PRIVACY

Pretty Good Privacy (PGP) is software that is used to encrypt e-mails. It was written by Philip Zimmerman, a software engineer and computer consultant, and released on June 5, 1991. As of 2019, PGP is the standard for encrypted e-mail worldwide (Open PGP, 2016a). In the fight on cybercrime, PGP has become both a sword and a shield. It is used by law enforcement to encrypt and protect their communications, but it is also used by cybercriminals to do the same (Leyden, 2006).

Attitudes toward PGP have shifted over the years. Following the initial release of PGP in 1991, there was a demand for e-mail encryption software. Zimmermann was solicited by volunteers to help work on PGP and to port it to other platforms. In September, 1992, PGP 2.0 was released. It contained some improvements and was available for numerous platforms and in numerous languages. The popularity of PGP—and its worldwide availability—appears to have caught the eye of law enforcement in the United States (Zimmermann, 2001). While there was public demand for encryption software, the government had concerns with its implementation. Around the time PGP was being written and released, the government had been advocating the implementation of encryption software that would permit the NSA a bypass around the encryption. The NSA wanted this in place so it could not be prevented from accessing data in instances where it had a warrant or other court order to obtain that data. PGP was not designed to permit this. Indeed, it appears Zimmermann may have created PGP in response to the government's proposal to require encryption to provide a bypass for the government (Stay, 1997).

In 1993, a federal investigation was opened to determine whether Zimmermann violated U.S. law by distributing PGP. The investigation involved the U.S. Customs Service. At the time, cryptographic software was considered a munition for purposes of the Arms Export Control Act. Thus, export of cryptographic software such as PGP to foreign countries could potentially have been considered a violation of this Act (Stay, 1997). The investigation in Zimmermann continued for three years. On January 11, 1996, the U.S. government closed the investigation without filing criminal charges against Zimmermann. The government provided no explanation why they closed the investigation (Zimmermann, 1996a). Since that time, encryption has become more commonplace. Government regulations may even require organizations to use encryption to not run afoul of information disclosure laws (Leyden, 2006). Nonetheless, the government's decision to not prosecute Zimmermann is not necessarily recognition that his actions were legal. Someone distributing cryptographic software to foreign countries in the United States could still potentially face legal repercussions (Zimmermann, 1996a).

Zimmermann no longer owns PGP. As noted above, he initially released PGP as freeware. After the criminal investigation was closed in 1996, he founded PGP Inc. which retained ownership of PGP. PGP Inc. was acquired by Network Associates Inc. in 1997. Network Associates developed PGP for both commercial and freeware uses. Network Associates sold the rights to PGP to PGP Corporation in 2002, and PGP Corporation was acquired by Symantec in 2010 (Open PGP, 2016b; Zimmermann, 2019). There are still encryption products that incorporate Open PGP standards—the open standards version of PGP that had been made available by Network Associates when they still controlled the rights to PGP (Open PGP, 2016b). Zimmermann appears to be a proponent of Open PGP products and vendors (Zimmerman, 2019).

See also: Bypass; Open-Source; Privacy

Further Reading

Leyden, John. 2006. "PGP creator: Net is like 'downtown Bagdad.'" *The Register*, November 21, 2006. https://www.theregister.co.uk/2006/11/21/pgp_at_15/

Open PGP. 2016a. "About." Open PGP. https://www.openpgp.org/about/

Open PGP. 2016b. "History." Open PGP. https://www.openpgp.org/about/history/

Stay, Ronald J. 1997. "Cryptic controversy: U.S. government restrictions on cryptography exports and the plight of Philip Zimmermann." *Georgia State University Law Review*13, 2: 581–604.

Zimmermann, Philip. 1996a. "Significant moments in PGP's History: Zimmermann case dropped." https://philzimmermann.com/EN/news/PRZ_case_dropped.html

Zimmermann, Philip. 1996b. "Testimony of Philip R. Zimmermann to the Subcommittee on Science, Technology, and Space of the US Senate Committee on Commerce, Science, and Transportation." https://philzimmermann.com/EN/testimony/index.html

Zimmermann, Philip. 2001. "PGP marks 10th anniversary." http://www.philzimmermann.com/EN/news/PGP_10thAnniversary.html

Zimmermann, Philip. 2019. "Where to get PGP." https://philzimmermann.com/EN/findpgp/

PREVENTION

Cybercrimes cannot be prevented, but there are ways to lessen the chance that a person or business will be the victim of an attack, making it more difficult for an offender to target a computer or system. They can do this through acting proactively or taking specific precautions to protect their computers to mitigate the impact of an event or weaken the consequences.

Cybercriminals will attack systems that have vulnerabilities or have weak security. Firewalls and virus protection software help prevent an unauthorized person from gaining access to a computer and thereby protect an individual from becoming a victim. This should be updated on a regular basis, and patches should be installed if provided. Another essential security measure that should be installed is some kind of intrusion detection that will notify the system owner or operator that a system has been breached. If possible, companies should hire a security expert to ensure all computers are protected at all times. All organizations should have a digital security policy in place for their agency that will assess threats and attacks. This should be reviewed regularly and updated if needed.

Another way to prevent cybercrimes is to increase public awareness of internet safety. This can be accomplished through formal education and/or professional training, which can provide users with ways on how to avoid becoming a victim. This is important because many people and employees have limited computer skills so it is difficult to do something. People should also be informed of the dangers of using pirated software, which can often include malware that can damage a computer system. All documents with private information should be shredded and not simply thrown away in a trash can.

Complicated passwords that are not simple or obvious are an easy way for individual users to protect their data. Users should not use the name of their child, spouse, or pet as a password. Instead, all passwords should be "strong passwords" that include at least eight characters, capital letters, numbers, and/or symbols. All passwords should be changed regularly, usually around every 90 days.

All computer users need to be educated so they can identify and recognize fake e-mails that may be an attempt at phishing (stealing personal information) or that may include malware. Fake e-mails often include an offer or deal that appears to be too good to be true, and it probably is. It is essential that people know not to click on links or open links that are not from a person they know. No employee or individuals should respond to e-mails or phone calls that require the caller to provide a password or other personal information, especially if it pertains to a bank account. Employees and individuals should be aware of any scams that are popular and how to avoid them.

By checking bank statements often, people and organizations will be able to recognize any suspicious or unrecognized activity. They can then report this anomaly quickly to a bank official.

Public Wi-Fi that is available to customers at restaurants, coffee shops, or hotels can be an easy way for cybercriminals to gain access to personal data. The connections at public Wi-Fi sites are often not secure, and criminals can easily steal passwords and other information.

It is important that all businesses, organizations, and individuals are prepared for an attack. This means that all essential data is backed up to prevent data loss but also so that it is available so the agency can continue to provide their services to clients or customers. They must also have a response plan in place in the event an attack does occur.

Restricting employee access to information is one way that companies and agencies can limit data theft. By limiting what information employees can access, they can limit the theft of data that could be harmful to the organization or individuals if made public. If an employee does not need access to particular data, they should be restricted from having access to it. Limiting employee access to databases during off hours or when they are not in the office is another effective method for protecting data. All staff should be required to return all equipment if they leave a company, including zip drives or external storage devices. New employees should be vetted so that they do not pose a threat to the security of the data they access.

Reporting suspicious activity on any account to either to an IT office or law enforcement agency immediately when it is discovered is imperative. If serious, the attack should be reported to a law enforcement agency such as the FBI or the Federal Trade Commission.

An incident response plan is necessary for all agencies and corporations in case they become the victim of a cyberattack. This way, if an attack occurs, employees know immediately what action to take. A quicker response may limit the damage done by an attack. The effects of the attack should be recorded, along with every action that the organization takes in response. It is critical that all evidence be preserve. Senior personnel in the agency should be notified. Immediate action should be taken to limit the extent of the problem needed.

In addition to these precautions for individuals and businesses, other precautions can assist in reducing cyberattacks. One is to procedures into place for effective sharing of information regarding the threats of cyberattacks or actual attacks if they occur. That way others can take actions to protect their systems, if need be. Moreover, law enforcement will benefit from additional evidence as they search for the offenders.

In a similar vein, all enforcement procedures should be applied similarly by all states. That way an offender cannot choose to commit a crime in a venue that has a lower penalty or punishment.

Law enforcement in all states need to have more training in cybercrime. Most departments are becoming more effective at fighting cybercrime. They are becoming more comfortable with the internet and technology, and there are more officers who have expertise and knowledge of technology. Some departments have placed officers in positions to pose as minors online as a way to catch predators and others seeking to harm users. Nonetheless, there are many agencies that need more officers who are trained in tracking down cybercrimes and cyberoffenders.

Prevention of cybercrime cannot be limited to an agency, business, or individual. Instead, a true attack on cybercrime must be international. Cybercriminals do not recognize national borders. A cyberattack can come from anywhere around the globe. This points to the importance of international treaties and agreements such as The Convention on Cybercrime that was negotiated by the Council of Europe. It is a true effort to improve the international enforcement of cybercrimes through creating similar laws between countries. It also increases the investigatory powers of law enforcement, increases the cooperation, and requires that police are available to help each other at any time.

It is essential that children who use the internet are protected as well. Adults should monitor what sites the child goes to and the time they spend on the sites. If they spend a longer time on some sites, it could indicate a problem and should be noted. If porn is found on a computer, it could be a possible sign that the child has had contact with a pedophile. Adults should be cautious if the child turns the computer monitor off quickly or changes the screen if an adult enters the room.

While it is impossible to prevent a cybercrime from occurring, precautions such as these can reduce the impact of a cyberattack or lessen the chances that an attack will occur.

See also: Council of Europe Cybercrime Convention; Cybersecurity; Password

Further Reading

Boyle, Randall J. 2013. *Corporate computer security*, MA. Boston: Pearson.

Brenner, Susan W. 2007. "Cybercrime: Re-thinking crime control strategies." In *Crime online*, edited by Yvonne Jewkes. Devon, UK: Willan Publishing, pp. 12–28.

Bryant, Robin, Bryant, Sarah. 2014. *Policing digital crime*. Farnham, Surrey: Ashgate.

Choi, Kyung-Shick. 2011. "Cyber-routine activities: Empirical Examination of online lifestyle, digital guardians and computer-crime victimization." In *Cyber criminology*, edited by K. Jaishankar. Boca Raton, FL: CRC Press, pp. 229–252.

McQuade, S.C. 2006. *Understanding and managing cyber crime*. Boston, MA: Pearson/Allyn and Bacon.

PRISM

Prism is a surveillance program in the United States that was launched by its government in 2007. The program is run by the NSA and is permitted under FISA. FISA was initially passed in 1978, though the rules governing it were relaxed in 2008, only requiring the NSA to show to a court that the information it wished to gather was for foreign intelligence purposes. Identifying the targets whose communications were to be monitored and verifying that those targets were outside the United States when those communications were made were no longer required (Kelion, 2013). These rules were renewed in 2012 (Greenwald and MacAskill, 2013). The stated purpose of the program is to gather information to aid in counterterrorism efforts (Associated Press, 2013; Parkinson, 2013).

The details of the Prism program came to light in 2013. The Prism program was included in the information leaked by Edward Snowden—a former NSA contractor—in June of that year. Prior to the leak, the existence of this program was not made known to the public. According to the leaked information, the servers of several large technology companies—Google, Facebook, Apple, Microsoft, and Yahoo, among others—were directly accessible by the NSA. The type of data the NSA is able to access is broad, including e-mails, photos, videos, chat logs, voice messages, social network details, and stored data (Greenwald and MacAskill, 2013). In response to the information leaked by Snowden, James Clapper—the director of National Intelligence at the time—declassified some aspects of the Prism program. Clapper noted that Prism cannot be used to target the communications of U.S. citizens, only foreign individuals. However, those communications may be unintentionally picked up in the collection process. In order to avoid inadvertent collection of such data, safeguards have been put in place. These include oversight by a special FISA court, training for personnel in the NSA using the Prism program, and regular congressional briefings on the program (Associated Press, 2013).

The technology companies involved with Prism gave varying answers in response to inquiries about their participation in the program. Some claimed they had never heard of Prism. Others indicated that they only provided information to the government is response to court orders to do so. These statements were vague, and not necessarily denials that the companies participated in the program (Stern, 2013). It appears the companies may have been prohibited by the government from mentioning the fact that they had complied with the Prism program. Indeed, following Snowden's leak of the Prism program, Yahoo requested that records be unsealed regarding a challenge it made to an information request it received from the NSA under the Prism program in 2007 (Hautala, 2016).

The documents leaked by Snowden also revealed that the United Kingdom had a similar surveillance program in place known as Tempora. The Tempora program was launched in 2011. The Government Communications Headquarters (GCHQ) in the United Kingdom placed interceptors on the fiber-optic cables entering the country, allowing it to monitor vast amounts of incoming data. Indeed, it appears the GCHQ has the widest access to surveillance information online (MacAskill et al., 2013; Shubber, 2013). Just as Prism was authorized in the United States under FISA, Tempora was authorized in the United Kingdom under the Regulation of Investigatory Powers Act (RIPA). RIPA appears to give GCHQ broad authority to intercept communications, being able to potentially intercept communications relating to terrorism and organized crime generally (Shubber, 2013). This information is accessible by NSA employees, with roughly 850,000 such employees and contractors having access to the GCHQ data (MacAskill et al., 2013). Where Tempora was capable of collecting data on U.S. citizens and the NSA had access to that data, there was concern that the United States may be reciprocating and providing data it obtained on United Kingdom citizens to GCHQ as a way for each government to circumvent the laws in their respective countries. In 2013, the Intelligence and Security Committee of Parliament in the United Kingdom found that data from Prism had been provided to the GCHQ, but that the GCHQ had been compliant with the law when obtaining that data.

The response to Snowden's leak of the Prism program was criminal charges. Should Snowden be extradited to the United States and he be convicted, he could face up to 30 years in prison (Kramer, 2017). In the United Kingdom, the GCHQ demanded that the *Guardian*—one of the two newspapers to first publish the Snowden leaks—either turn over or destroy the information that Snowden had provided to them. To avoid ultimately handing the information over to the GCHQ, the *Guardian* ultimately destroyed the hard drives on which the information was contained, with technicians from GCHQ witnessing the event (Borger, 2013).

As mentioned above, the initial reason stated justifying the existence of the Prism program was that it is necessary to aid in counterterrorism efforts. Gen. Keith Alexander—director of the National Security Administration at the time Snowden leaked information on Prism—claimed that Prism was responsible for thwarting over 50 terrorist attacks around the world. Only a few examples of attacks prevented by Prism were provided by Alexander. This included a plot by Najibullah Zazi to bomb the New York subway system in 2009 (Parkinson, 2013). In Zazi's case, there is some question whether Prism was truly necessary to foil the plot. It appears that in Zazi's case, a warrant had been obtained to monitor his e-mail communications, and thus the communications would have arguably been available to the NSA whether Prism was in place or not (Apuzzo and Goldman, 2013).

The Prism program was renewed in 2018. An amendment to the program was considered wherein the NSA would have to get a warrant to query the database that contained intercepted communications under the program. However, the program was renewed without that amendment (Hautala, 2018).

See also: International Issues; Privacy; Snowden, Edward

Further Reading

Apuzzo, Matt, and Adam Goldman. 2013. "NYC bomb plot details settle little in NSA debate." *Omaha World-Herald*, June 11, 2013. https://www.omaha.com/news/nyc-bomb-plot-details-settle-little-in-nsa-debate/article_ecf63d66-715a-5744-8152-27c679abf957.html

Associated Press. 2013. "Intelligence chief blasts NSA leaks, declassifies some details about phone program limits." Fox News, June 6, 2013. https://www.foxnews.com/us

/intelligence-chief-blasts-nsa-leaks-declassifies-some-details-about-phone-program-limits

Borger, Julian. 2013. "NSA files: Why the *Guardian* in London destroyed hard drives of leaked files." *The Guardian*, August 20, 2013. https://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london

Greenwald, Glenn and Ewen MacAskill. 2013. "NSA Prism program taps in to user data of Apple, Google and others." *The Guardian*, June 7, 2013. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Hautala, Laura. 2016. "The Snowden effect: Privacy is good for business." CNet, June 3, 2016. https://www.cnet.com/news/the-snowden-effect-privacy-is-good-for-business-nsa-data-collection/

Hautala, Laura. 2018. "NSA surveillance programs live on, in case you hadn't noticed." *CNet*, January 19, 2018. https://www.cnet.com/news/nsa-surveillance-programs-prism-upstream-live-on-snowden/

Intelligence and Security Committee of Parliament. 2013. "Statement on GCHQ's alleged interception of communications under the U.S. PRISM programme." http://isc.independent.gov.uk/committee-reports/special-reports

Kelion, Leo. 2013. "Q&A: NSA's Prism internet surveillance scheme." *BBC*, June 25, 2013. https://www.bbc.com/news/technology-23027764

Kramer, Andrew E. 2017. "Russia extends Edward Snowden's asylum." *New York Times*, January 18, 2017. https://www.nytimes.com/2017/01/18/world/europe/edward-snowden-asylum-russia.html

MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies, and James Ball. 2013. "GCHQ taps fibre-optic cables for secret access to world's communications." *The Guardian*, June 21, 2013. https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

Parkinson, John R. 2013. "NSA: 'Over 50' terror plots foiled by data dragnets." *ABC News*, June 18, 2013. https://abcnews.go.com/Politics/nsa-director-50-potential-terrorist-attacks-thwarted-controversial/story?id=19428148

Shubber, Kadhim. 2013. "A simple guide to GCHQ's internet surveillance programme Tempora." *Wired*, June 24, 2013. https://www.wired.co.uk/article/gchq-tempora-101

Stern, Joanna. 2013. "Dissecting big tech's denial of involvement in NSA's PRISM spying program." *ABC News*, June 7, 2013. https://abcnews.go.com/Technology/nsa-prism-dissecting-technology-companies-adamant-denial-involvement/story?id=19350095

PRIVACY

As technology advances and services increasingly move online, privacy increasingly becomes a concern. With regard to cybercrime, privacy becomes an issue in two ways. First, there is information people wish to keep private that cybercriminals may attempt to discover. This can include personally identifying information such as social security numbers, birthdates, and login credentials for online financial and other accounts. Maintaining privacy from cyberattacks thus becomes a concern. Second, from a law enforcement standpoint, the privacy rights of individuals must be observed when conducting an investigation. Failure to abide by the rules designed to protect these rights may negatively affect an investigation, potentially preventing the successful prosecution of a cybercriminal.

There are several ways cybercriminals can invade the privacy of others. Cybercriminals often attempt to obtain the personally identifying information of victims in order to use that information for financial gain. The information itself is something victims generally wish to keep private. Nonetheless, victims will sometimes voluntarily disclose this personal information to cybercriminals under false pretenses. This may be done as part of a social engineering attack by a cybercriminal—an attack whereby the cybercriminal solicits private information from a victim by pretending to be someone who would have a legitimate reason to obtain the information from the victim. For example, a cybercriminal could pretend to be a bank employee and call the victim under the pretense that the victim needs to verify their online account information with the employee. Other privacy breaches can occur through the use of malware. Some malware is designed to gain access to the private information of a victim. This would include spyware, sniffers, and keystroke monitors.

With cybercrime, privacy can exponentially erode once an initial breach of privacy has occurred. Once a cybercriminal obtains private information from a victim, they can then use that information to access further personal information. If bank information is obtained, the cybercriminal gains access to the victim's private financial information. If e-mail login credentials are obtained, a cybercriminal can scour the victim's e-mails to find more personal information. A cybercriminal might even use a victim's e-mail account to engage in phishing, sending e-mails to the victim's contact list either as part of a social engineering attack or in attempts to get these subsequent victims to click on a link in the e-mail that will download spyware or other privacy-invasive malware. If a cybercriminal is able to obtain personally identifying information from those subsequent victims, the cybercriminal can theoretically repeat this process in perpetuity until they are caught.

Even if people take the proper precautions to avoid falling victim to phishing, social engineering, and other attacks designed to obtain their personally identifying information, cybercriminals may still obtain it if others entrusted with that information fall victim to such an attack. This can been seen with data breaches that several companies experience. Several large companies—including Yahoo, Sony, Target, and eBay—have been the victims of data breaches (Baker and Finkle, 2011; Larson, 2017; McCoy, 2017; Wakefield, 2014). Millions of customers' data—billions in the case of Yahoo—was stolen in these incidents. People can be proactive when deciding which organizations to provide personal information to, reviewing the organization's privacy policies and data retention policies prior to providing it to an organization. However, even this may not completely shield someone from having their private data accessed by cybercriminals. An example of this is the hack of the Ashley Madison website. Ashely Madison was a website designed to facilitate marital affairs. In 2015, a hacker group known as the Impact Team was able to steal customer information and reveal it online. The group's motivation was its opposition to the company's practice of retaining customer information despite having a policy to not do so (Thomsen, 2015). Thus, a customer who used the services of Ashley Madison and relied on the company's representation of the data retention policy may have had their private information publicly disclosed as part of this breach. In some instances, an organization may have someone's personal information, and the person may not be aware of it. This can be seen in the Equifax data breach. Equifax is a credit reporting agency. As such, it is legally able to obtain the credit information of people for the purpose of constructing a credit score, and that score is shared with authorized entities when needed, such as when someone applies for a credit card or seeks a car loan. Credit reporting agencies gather this information whether or not a person wants it to be gathered. In 2017, Equifax suffered a data breach. Approximately 145 million people had their information taken (Kennedy, 2018; Regnier and Woolley, 2017).

Privacy is also a concern that law enforcement must be aware of when investigating crimes—cybercrimes included. In the United States, there are rules that dictate what law enforcement must do in order to gain access to an area wherein an individual has an expectation of privacy. This generally requires that law enforcement obtain a warrant before searching such an area or seizing any property from that area. In the cybercrime context, this could apply to digital evidence on a computer or other electronic device, as well as digital evidence contained in e-mail or other online accounts. With e-mail and other online accounts, one factor that may have an impact on whether a person should expect the information in those accounts to be private is the privacy policies of the companies hosting those accounts. Privacy policies will generally include language that indicates the company will disclose information to law enforcement when it is legally required to do so—such as when a warrant is served on it. Those same policies may also cast a broader net, noting that the company will provide information to law enforcement if the company determines it is necessary to prevent harm to itself (Facebook, 2019; Google, 2019). Additionally, it appears there may be times when technology companies have had to disclose information to law enforcement without divulging the nature of that disclose to its users (Hautala, 2018). This came to light after Edward Snowden—a former NSA contractor—publicly leaked information about Prism, an NSA program that gathered data from technology companies such as Microsoft, Facebook, Apple, Yahoo, and Google (Burrough and Ellison, 2014; Greenwald and MacAskill, 2013). Following Snowden's leak in 2013, it came to light that Yahoo had opposed disclosing information to the NSA as part of Prism in 2007 (Hautala, 2016).

There are online tools that people can use to potentially increase the privacy of their information. Large technology companies seek to assure users that their services are secure and that user information will remain private. In the wake of Snowden's leaks, these companies appear to have doubled down on such assurances to customers (Hautala, 2016). There are other tools that people have turned to for increased online privacy. Some people use virtual private networks (VPNs) and the Tor web browser to maintain privacy in their online activity. Some may use cryptocurrencies, such as Bitcoin, to maintain privacy in their online purchases. While these tools can certainly help people attain some additional privacy in their online activity, they are not perfect. VPNs and Tor can only maintain privacy for a user to the extent that the people running them decide to maintain that privacy (Dinha, 2019; Franceschi-Bicchierai, 2015). Cryptocurrencies do add an additional layer of privacy to customers using them, but cryptocurrency transactions are still able to be traced by law enforcement and others with the proper tools.

See also: Bitcoin; Cryptocurrency; Keystroke Monitoring; Malware; Personally Identifying Information; Phishing; Sniffer; Snowden, Edward; Social Engineering; Spyware; State Actor; Tor (The Onion Router); Virtual Private Network

Further Reading

Baker, Liana B., and Jim Finkle. 2011. "Sony PlayStation suffers massive data breach." *Reuters*, April 26, 2011. https://www.reuters.com/article/us-sony-stoldendata/sony-playstation-suffers-massive-data-breach-idUSTRE73P6WB20110427

Burrough, Bryan and Sarah Ellison. 2014. "The Snowden saga: A shadowland of secrets and light." *Vanity Fair*, April 23, 2014. https://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview

Dinha, Francis. 2019. "The mistakes you're making with your VPN." *Forbes*, March 29, 2019. https://www.forbes.com/sites/forbestechcouncil/2019/03/29/the-mistakes-youre-making-with-your-vpn/#2bb2c07b67cd

Facebook. 2019. "Data policy." https://www.facebook.com/policy.php

Franceschi-Bicchierai, Lorenzo. 2015. "A researcher used a honeypot to identify malicious tor exit nodes." Motherboard, June 26, 2015. https://motherboard.vice.com/en_us/article/mgbdwv/badonion-honeypot-malicious-tor-exit-nodes

Google. 2019. "Google privacy policy." https://policies.google.com/privacy?hl=en#infosharing

Greenwald, Glenn and Ewen MacAskill. 2013. "NSA Prism program taps in to user data of Apple, Google and others." *The Guardian*, June 7, 2013. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data on January 17, 2019.

Hautala, Laura. 2016. "The Snowden effect: Privacy is good for business." *CNet*, June 3, 2016. https://www.cnet.com/news/the-snowden-effect-privacy-is-good-for-business-nsa-data-collection/

Hautala, Laura. 2018. "NSA surveillance programs live on, in case you hadn't noticed." *CNet*, January 19, 2018. https://www.cnet.com/news/nsa-surveillance-programs-prism-upstream-live-on-snowden/

Kennedy, Merit. 2018. "Equifax says 2.4 million more people were impacted by huge 2017 breach." National Public Radio, March 1, 2018. https://www.npr.org/sections/thetwo-way/2018/03/01/589854759/equifax-says-2-4-million-more-people-were-impacted-by-huge-2017-breach

Larson, Selena. 2017. "Every single Yahoo account was hacked—3 billion in all." CNN, October 4, 2017. https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html

McCoy, Kevin. 2017. "Target to pay $18.5M for 2013 data breach that affected 41 million consumers." *USA Today*, May 23, 2017. https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/

Regnier, Pat, and Suzanne Woolley. 2017. "Thank you for calling Equifax. Your business is not important to us." Bloomberg, September 14, 2018. https://www.bloomberg.com/news/features/2017-09-14/thank-you-for-calling-equifax-your-business-is-not-important-to-us

Thomsen, Simon. 2015. "Extramarital affair website Ashley Madison has been hacked and attackers are threatening to leak data online." *Business Insider*, July 20, 2015. https://www.businessinsider.com/cheating-affair-website-ashley-madison-hacked-user-data-leaked-2015-7

Wakefield, Jane. 2014. "eBay faces investigations over massive data breach." BBC, May 23, 2014. https://www.bbc.com/news/technology-27539799

PROFITS FROM CYBERCRIME

Cybercrime provides high returns with a low risk for offenders. There is a significant amount of money that can be made through the commission of crimes committed via the internet. When it comes to cybercrimes, there are very low costs with a potentially very large profit, and few offenders are caught and punished for the acts. It has been estimated that the total global impact of cybercrime is around $3 trillion (Khimji, 2015).

It is often difficult to track the source of a cyberattack. The offender(s) could be located in a different country where the laws are different, and cooperation with law enforcement may be difficult. Offenders are well organized and know what they want or need to do. Many cyber-attacks are committed by highly organized international crime groups, many of whom have developed relationships with drug cartels and terrorist cells (Dethlefs, 2015). Cybercriminals are often able to carry out an attack and move to a different location to evade authorities.

Because so many cybercrimes go unreported, it is difficult to know the exact costs of these crimes. Company officials either choose not to report a crime because they fear the effect it could have on their business, or they may be unaware that an attack occurred. Cybercrime has become a cost of doing business; they occur often and have a major impact on businesses. In 2013, the U.S. government notified 3,000 companies that they had been hacked (Center for Strategic Studies, 2014).

For companies, especially small companies, a cyberattack can be devastating. The average cost of a corporate data breach is estimated to be about $5.9 million, and the cost of lost business from a breach averages $3.2 million (Dethlefs, 2015). A report by Hewlett Packard and Ponemon Institute of Cybercrime indicates that the average American firm pays $15.4 million a year on hacking attacks (Ponemon, 2016). Companies have to pay for preventative measures to lessen the chances that they will become a victim, such as improving security. In the event that an attack occurs, companies may suffer loss of financial assets. They will also have to pay costs of recovering from the attack and costs related to damage done to the company's reputation. The costs of recovering from attacks is increasing as the attacks become more common and more complex.

Cybercrime has become more profitable than global trade in drugs, including marijuana, cocaine, and heroin combined (Khimji, 2015). The revenues from cybercrime are often greater than revenues from legitimate small or mid-size companies. Profits from cybercrime are estimated to be about $200 billion every year (McGuire, 2018). This comprises general earnings from illicit and illegal online sales of goods ($860 billion), intellectual property theft ($500 billion), data trading

($160 billion), crimeware-as-a-service ($1.6 billion), and ransomware ($1 billion) (McGuire, 2018). Put another way, if cybercrime were a country, it would have the 13th-highest gross domestic product (GDP) in the world. Individually, it is estimated that an average hacker will earn around $30,000 a year from their activities.

There is no doubt that the costs of cybercrime will increase in the future. An increasing number of businesses rely on the internet for sales and customer relations. In addition, more consumers are purchasing goods online. The increase in retail marketing and sales opens up more opportunities for theft and fraud. Moreover, it is becoming easier to launch an attack. Cyber criminals can easily purchase the software needed to carry out a cybercrime—they do not need to know how to write it themselves. To make matters worse, the average price of launching a distributed DDoS attack has decreased recently. It now will cost an offender about $38 per hour to carry out an attack (Griffiths, 2015).

It is essential that information on cyber threats and crimes is collected and tracked in order to watch trends, and also to possibly prevent attacks. In some countries, companies are not required to report data breaches when they occur, so many companies will not contact officials. They don't want the public to know about a possible breach. This means that the data regarding crimes is incomplete and inaccurate. In order to improve policies and response to crimes, all offenses must be reported.

See also: Economy, Effects on; Distributed Denial-of-Service Attack (DDoS); Identity Theft

Further Reading

Ashford, Warwick. 2018. "Global cyber crime worth $1.5tn a year, study reveals." *Computer Weekly*, April 20, 2018. https://www.computerweekly.com/news/252439584/Global-cyber-crime-worth-15tn-a-year-study-reveals

Center for Strategic and International Studies. 2013. "The economic impact of cybercrime and cyber espionage." https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf

Center for Strategic and International Studies. 2014. "Net losses: Estimating the global cost of cybercrime." https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/McAfee%20and%20CSIS%20-%20Econ%20Cybercrime.pdf

Dethlefs, Robert. 2015. "How cyber attacks became more profitable than the drug trade." *Fortune*, May 1, 2015. http://fortune.com/2015/05/01/how-cyber-attack-became-more-profitable-than-the-drug-trade/

Griffiths, James. 2015. "Cybercrime costs the average U.S. firm $1 million a year." CNNMoney, October 8, 2015 http://money.cnn.com/2015/10/08/technology/cybercrime-cost0byusinessindex.html.

Khimji, Irfahn. 2015. "State of security." TripWire, March 30, 2015. https://www.tripwire.com/state-of-security/regulatory-compliance/pci/cybercrime-is-now-more-profitable-than-the-drug-trade/

McGuire, Mike. 2018. "Webstresser: When platform capitalism goes rogue." Bromium, July 13, 2018. https://www.bromium.com/webstresser-when-platform-capitalism-goes-rogue/

Ponemon Institute. 2016. “Cost of cyber crime study & the risk of business Innovation.” Sponsored by Hewlett Packard Enterprise. https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf

PUBLIC DOMAIN

The public domain refers to the body of creative works whose intellectual property protections are no longer in effect. In the United States, intellectual property protections include the exclusive rights to reproduce and distribute the creative work. Once a creative work enters the public domain, it can be reproduced and distributed freely by anyone.

If someone believes a creative work is in the public domain when it is not in fact in the public domain, they could be liable for violating the author’s intellectual property rights if they use that work. On the internet, this can sometimes happen. There are websites that claim creative works (pictures, audio, video) on their site are in the public domain and that anyone can use them free of charge. An example would be the site Pexels. Users of that site can upload pictures for others to download. The terms of service require that users only upload pictures that are in fact in the public domain or pictures taken by the user that they are releasing into the public domain (see Pexels, 2019). A user who is determined to put up pictures still covered by copyright, however, could still post them. Subsequent users of the site who then download those pictures could be liable for using the pictures without having paid for them.

Issues with the public domain can affect websites that sell pictures online as well. Getty Images is one such website. Getty Images encountered legal troubles in 2016 after they sent a letter to Carol Highsmith—an accomplished photographer—demanding that she remove a photograph from her website. Getty Images claimed the photograph was one they owned the copyright to and that Highsmith owed them money. In reality, the photograph was one that Highsmith had taken herself and released to the public domain. Because of this letter, Highsmith discovered that Getty Images was using the photographs she released to the public domain and was charging people for them (Sullivan, 2016). Thus, on the internet, users run the risk of not only violating someone’s intellectual property rights unintentionally when they mistakenly download pictures and other creative works that end up not being in the public domain, but they also run the risk of paying for material that is rightfully in the public domain.

A work generally enters the public domain in one of two ways. First, the time period specified by law within which the work is entitled to protection could expire. The length of time that a creative works receives intellectual property protection depends on the work in question. For works covered by copyright law—books, songs, movies, and pictures, among others (see 17 U.S. Code § 102)—the author of those works generally maintains copyright protection for those works for the duration of his or her life, plus 70 years (17 U.S. Code § 302). For works covered by patent law—namely inventions (see 35 U.S. Code § 101)—the inventor maintains patent protection for 20 years (35 U.S. Code § 154). Works created by the U.S. government that would normally be eligible for copyright protection are immediately released to the public domain (17 U.S. Code § 105). However, the government may still seek patent protection for its inventions.

The second way a creative work enters the public domain is when the owner of the intellectual property rights waives those rights. It is possible for the owner of intellectual property rights to only waive some of those rights, or waive those rights with restrictions. For example, an artist might design several graphics for people to use, as long as the graphics are used for non-commercial purposes. In a situation like this, the graphics would not be in the public domain. It is only where a creative work is completely unencumbered by intellectual property right restrictions that it would be in the public domain.

Creative Commons is an organization that assists the authors of creative works with sharing those works in a fashion that retains only some of the author's intellectual property rights or completely releases the work into the public domain. Creative Commons provides varying licenses that authors may include with their creative work. Those licenses specify the rights the author wishes to retain and which rights the author wishes to relinquish. Creative Commons is not necessary to waive one's intellectual property rights. An author of a work can release their individual intellectual property rights in any way they see fit. Creative Commons simply provides a medium that authors can use to easily clarify the intellectual property right status of their work.

Examples of creative works with expired intellectual property protections would be the writings of Edgar Allan Poe, William Shakespeare, and Mark Twain. An example of creative works with waived intellectual property rights would be the electric vehicle patents owned by Tesla Motors, which were waived by the company in 2014 (see Musk, 2014).

See also: Abandonware; Copyright Infringement; Open-Source

Further Reading

Creative Commons. 2018. "Creative Commons master terms of use." https://creativecommons.org/terms/ on October 9, 2018.

Musk, Elon. 2014. "All our patent are belong to you." Tesla Motors, June 12, 2014. https://www.tesla.com/blog/all-our-patent-are-belong-you

Pexels. 2019. "Terms and conditions." Pexels. https://www.pexels.com/terms-of-service/

Sullivan, Bryan. 2016. "Getty likely to settle $1b suit by photographer for appropriating her public-domain work." *Forbes*, August 3, 2016. https://www.forbes.com/sites/legalentertainment/2016/08/03/pay-up-getty-sends-trolling-letter-to-photographer-highsmith-demanding-money-for-her-own-photos/#1b9e9627596e

PUNISHMENT

Convictions for cybercrimes come with the same forms of punishment as other crimes do. The imposition of fines, a term of probation, or a term of incarceration are all possibilities. In the United States, both the federal government and state government can regulate cybercrimes.

Many crimes became easier to commit following the advent of the internet. Criminals took advantage of a bevy of new methods the internet provided. For example, while the possession of child pornography, intellectual property theft, and financial crimes were already outlawed prior to the internet, new technology created new methods for these crimes to be committed, or more difficult to trace and prosecute. Criminals only need to download and share digital files to circulate child pornography or stolen intellectual property. For those looking to commit fraud and financial crimes, the internet provides a level of anonymity that face-to-face transactions do not, giving cybercriminals an advantage when trying to gain the trust of victim.

There are cybercrimes that are unique. Several jurisdictions have laws punishing the unauthorized access to a computer, or the intentional damage to a computer via malware or some similar mechanism. There are other crimes that could have technically taken place without the internet, but generally did not. An example of this would be revenge porn—the publishing of sexually explicit photographs of another without their permission. Someone could have received an actual photograph of their partner before the advent of the internet and then made numerous copies of that picture to post around town after they ended their relationship with their partner. This was not generally done, however. With the internet, posting of revenge porn is much easier. By posting a picture in a social media account, the picture could be viewed by virtually anyone and everyone.

Not all illegal cyberactivities would be crimes. There are many illegal activities that are punishable under civil law, resulting in a civil punishment such as an injunction, restitution, payment of fines, and so forth. Cybersquatting is an example of this. Cybersquatting is not a crime, but those who cybersquat can be required to relinquish the domain name on which they cybersquatted and pay a fine. Some illegal cyberactivities may have both a criminal and civil component to them, exposing the cybercriminal to two potential avenues of punishment. Intellectual property theft falls into this category. It is a crime to commit intellectual property theft, but the owner of the stolen intellectual property in question can also proceed against the thief civilly to recover the money they were deprived due to the theft (see United States Code).

Where cybercrimes are a relatively new body of crimes, judges can have a difficult time determining what an appropriate punishment is for a convicted cybercriminal. In the United States, there are sentencing guidelines for judges, though those guidelines can be quite broad. It appears judges are largely still in the transitionary stage with little precedent to rely upon (Williams, 2016).

There can be punishment for cyberactivity outside of an officially imposed government punishment. Many websites have regulations that prohibit harmful activity on their sites. While this certainly includes criminal activity such as the posting of revenge porn (Facebook, 2018; Instagram, 2018), it can also include prohibitions on cyber activity that is not illegal, such as doxing (Reddit, 2018; Twitter, 2018). Punishment in these instances could include being banned from the website in question. If the activity was also a violation of the law, the matter could be referred to law enforcement, and the perpetrator could face official government punishment in addition to the punishment meted out by the website.

See also: Child Pornography; Copyright Infringement; Cybersquatting; Doxing; Drug Trafficking; Financial Crimes; Fraud; Identity Theft; Malware; Money Laundering; Revenge Porn; Sexting

Further Reading

Facebook. 2018. "Not without my consent." https://fbnewsroomus.files.wordpress.com/2017/03/not-without-my-consent.pdf

Instagram. 2018. "What should I do if someone shares an intimate photo of me without my permission?" https://help.instagram.com/1769410010008691?helpref=search&sr=1&query=revenge%20porn

Reddit. 2018. "Is posting someone's private or personal information okay?" https://www.reddithelp.com/en/categories/rules-reporting/account-and-community-restrictions/posting-someones-private-or-personal

Twitter. 2018. "About private information on Twitter." https://help.twitter.com/en/rules-and-policies/personal-information

Williams, Katie Bo. 2016. "Judges struggle with cyber crime punishment." *The Hill*, January 19, 2016. https://thehill.com/policy/cybersecurity/265285-judges-struggle-with-cyber-crime-punishment

RANSOMWARE

Ransomware is a type of malware that cybercriminals use to extort money from computer users. A cybercriminal will access and take control of a computer or network. A user will be unable to access their files, including pictures, spreadsheets or other documents. The criminal will either lock the files, so the user is unable to access them unless payment is received, or the criminal will threaten to destroy the data if the money is not sent. Criminals may also threaten to release private data or confidential data unless payment is received. In most cases the offender will give the victim anywhere from 48 to 72 hours to respond to the threat and provide the payment. After the time has run out, the cost of the payment may increase or the data is destroyed. If the ransom is paid, the offender will send the victim a key to decrypt the files. The payment is typically in Bitcoins or other cryptocurrency rather than cash.

If a cybercriminal attacks a computer and blocks a user from accessing files unless money is paid, it is considered to be a form of cyberextortion. It can also by cyberextortion even if the offender threatens an attack unless money is paid. It is a form of traditional blackmail.

The use of ransomware is becoming more popular. One reason for this is that offenders are able to either purchase or rent a ransomware kit online for relatively cheap—somewhere between $10 and $1,800, depending on the quality of the kit. Many programs allow the criminal to choose the amount of ransom they will charge a victim so they can access their data (Sharp, 2017). Attacks on hospitals and police departments have increased as well because they often have critical files that are not backed up regularly, making them easy targets for extortion. In the end, offenders are rarely found and typically get away with their attacks undetected. They often operate outside of the United States where it is difficult for law enforcement to locate them.

In the United States, it is estimated that between 40 and 64 percent of those whose computers are affected by ransomware will pay the criminals to get access to their systems (Sharp, 2017). Individuals who have their personal computers infected often have not adequately backed up their files so if their computer is locked, they will lose files, records, and photos. They often pay the ransom in order to get these files back. Some companies, for example police and medical facilities, will pay the ransom because they need immediate access to files and don't have the time to try to recreate files. In 2016, the majority of ransomware attacks (69%) were carried out on private individuals; the rest were aimed at companies (Sharp, 2017).

It should be remembered that even if a victim pays the ransom to regain access to files, the offender may have seen and possibly retained, a copy of the files or other data they have stolen. So just because the ransom has been paid, it does not mean the victim is safe. The offender may also have enough information to steal the victim's identity or access bank accounts.

One popular ransomware program is called Cryptolocker, which first appeared in 2013. This program encrypted a user's files, making them unreadable without a key. Cybercriminals used Cryptolocker to infect tens of thousands of computers and extort $30 million from businesses in about three months (Jarvis, 2014). Agents at the U.S. Department of Justice shut down the attack through Operation Tovar. U.S. agents worked in cooperation with agents from Europol and the U.K. National Crime Agency. At the end of the investigation, Russian cybercriminal Evgeniy Mikhailovich Bogachev was arrested and indicted on 14 counts of conspiracy, computer hacking and fraud. After his arrest, security experts were able to provide victims with software keys so that they could unlock their data and access their files.

Many ransomware programs were developed in 2014 and caused havoc for users. One of these was CryptoWall, and the others were called TorrentLocker and CTB-Locker. These were sent to victims through spam e-mails that appeared to be legitimate. When the user clicked on the e-mail, the malware was uploaded, locking the files. In 2017, cybercriminals carried out a worldwide attack using a program called WannaCry. Like all ransomware, this program locked files and demanded payment in Bitcoins from victims if they wanted their files unlocked. The program attached itself to computers that had not installed an earlier security patch. Within a short time of the malware's release, Microsoft issued a new patch, preventing the further spread of the malware. Many countries, including the United States, accused North Korea of advancing the attack.

Cybersecurity companies have developed methods to decrypt files that have been locked. Many were developed after CryptoLocker caused a great deal of damage around the world. However, cybercriminals still use other ransomware programs to extort victims.

Cybersecurity firms recommend that users always verify websites they visit are legitimate, and avoid opening e-mails from unfamiliar sources. Backing up files regularly can also limit the data lost in an attack.

See also: Cryptocurrency; Encryption; Exploit Kit; Ransomware

Further Reading

Ahn, Gail-Joon, Doupe, Adam, Zhao, Ziming, and Liao, Kevin. 2017. "Ransomware and cryptocurrency: Partners in crime." In *Cybercrime through an interdisciplinary lens*, edited by Thomas Holt. New York: Routledge, pp. 105–126.

Fung, Brian. 2017. "How to protect yourself from the global ransomware attack." *Washington Post*, May 15, 2017. https://www.washingtonpost.com/news/the-switch/wp/2017/05/15/how-to-protect-yourself-from-the-global-ransomware-attack/?utm_term=.79f16ac2ba68

Jarvis, K. 2014. "Cryptolocker ransomware, 2013." www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware.

Sharp, Alastair. 2017. "Cyber extortion demands surge as victims keep paying: Symantec." *Reuters*, April 26, 2017. https://www.reuters.com/article/us-cyber-ransom/cyber-extortion-demands-surge-as-victims-keep-paying-symantec-idUSKBN17S1U6.

REPUTATION, EFFECTS ON

One of the harms that can be inflicted on victims of cybercrime is reputational harm. The type of harm suffered by human victims differs from the harm suffered by organizational victims. Cybercrime can also have an effect on the reputation of the cybercriminals that commit it.

Reputational harm to people based on online activity is a widely-shared concern. One study found that just under half (45%) of people believed that one's reputation could not recover from negative information posted online—be that posting the result of criminal activity or otherwise (Norton, 2010). There are some cybercrimes where the harm is specifically the posting of information harmful to another person. This includes revenge porn and the related crime of sextortion. Revenge porn is where a cybercriminal makes sexually explicit photographs or video of someone else available online without that person's permission. Sextortion is where a cybercriminal threatens to post revenge porn of someone unless that person pays the cybercriminal or otherwise provides them something of value. If such photographs or video is posted online, it can damage the reputation of the person depicted in those photographs or that video. Just the fact that pictures or video depicting the victim in such a fashion exists can potentially damage the reputation of the person depicted. One study found that only one-third of victims of sextortion told anyone that they had been so victimized, and even fewer—only 16 percent—reported the incident to law enforcement (Wolak and Finkelhor, 2016). Among the reasons given for this lack of reporting are shame and embarrassment.

Another online behavior that, by itself, is not necessarily criminal but can lead to criminal activity (and reputational harm) is doxing. Doxing is where someone posts online the personally identifying information of someone else, such as their contact information. Doxing can harm the reputation of the person targeted. This can be seen in the incident known as Gamergate, which started in 2014. As part of this incident, several women were doxed by hackers. As a result of the doxing, these women received death threats and threats of rape (McDonald, 2014; Quinn, 2017). Their reputations were also tarnished. For example, the reputation of Zoe Quinn—an independent video game developer doxed as part of Gamergate—suffered after allegations were leveled against her that she slept with a video game reviewed to improve the review given to her game (Quinn, 2017).

Organizations can also suffer reputational harm if they are the victims of cybercrime. Much as doxing can result in reputational harm for a human victim, leaked information can also cause reputational harm for an organizational victim. This can be seen with Edward Snowden's leak of the Prism program to the public. Under the Prism program, the NSA is able to collect information from technology companies that it feels will be helpful in counterterrorism efforts. According to the leaks by Snowden, the NSA had direct access to the servers of several large technology companies, such as Microsoft, Apple, Google, and Yahoo. The reputation of the NSA was impacted by this revelation, as were the reputations of the technology companies who were seen to be cooperating with the NSA. Those companies took measures to try and assure customers that customer privacy was a key concern for them as a means to rehabilitate that reputation (Hautala, 2016).

As can be seen in the example above, for business victims, reputational harm can result in actual economic harm for them. It is not just information leaks that cause this problem for business victims. Cyberattacks in general cause problems for business victims as well. When a business suffers a cyberattack, it may gain a reputation for being vulnerable to attacks, which can lower consumer confidence in that business. Cyberattacks can lower the valuation of a business and its stock prices (Bose and Leung, 2014; Goel and Shawky, 2009; Pirounias et al., 2014; Spanos and Angelis, 2014).

Commission of cybercrime can also have an impact on one's reputation. Those who are convicted of crimes—cybercrimes included—face the stigma of being labeled a criminal. However, with cybercrime, the level to which this stigma attaches can vary from country to country. One study found that cybercriminals are less likely to be stigmatized in countries were internet accessibility is low and the resources devoted to fighting cybercrime are low (Kshetri, 2010). In some countries, express or tacit approval of cybercrime may have an impact on the level of reputational harm suffered by cybercriminals. For example, China has policies in place that appear to encourage intellectual property theft by its citizens (Commission on the Theft of American Intellectual Property, 2017). In Russia, cybercriminals appear to be able to avoid apprehension as long as they focus their criminal efforts on foreign targets (Maurer, 2018).

See also: China; Copyright Infringement; Doxing; Personally Identifying Information; Prism; Revenge Porn; Russia; Snowden, Edward

Further Reading

Bose, Indranil, and Alvin Chung Man Leung. 2014. "Do phishing alerts impact global corporations? A firm value analysis." *Decision Support Systems* 64: 67–78.

Commission on the Theft of American Intellectual Property. 2017. "Update to the IP Commission Report." http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf

Goel, Sanjay, and Hany A. Shawky. 2009. "Estimating the market impact of security breach announcements on firm values." *Information & Management* 46: 404–410.

Hautala, Laura. 2016. "The Snowden effect: Privacy is good for business." CNet, June 3, 2016. https://www.cnet.com/news/the-snowden-effect-privacy-is-good-for-business-nsa-data-collection/

Kshetri, Nir. 2010. "Diffusion and effects of cyber-crime in developing economies." *Third World Quarterly* 31, 7: 1057–1079.

Maurer, Tim. 2018. "Why the Russian government turns a blind eye to cybercriminals." *Slate*, February 2, 2018. https://slate.com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals.html

McDonald, Soraya Nadia. 2014. "'Gamergate': Feminist video game critic Anita Sarkeesian cancels Utah lecture after threat." *Washington Post*, October 15, 2014. https://www.washingtonpost.com/news/morning-mix/wp/2014/10/15/gamergate-feminist-video-game-critic-anita-sarkeesian-cancels-utah-lecture-after-threat-citing-police-inability-to-prevent-concealed-weapons-at-event/?utm_term=.47212285ba0b

Norton. 2010. "Cybercrime report: The human impact." Symantec. https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf

Pirounias, Sotirios, Dimitrios Mermigas, and Constantinos Patsakis. 2014. "The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study." *Journal of Information Security and Applications* 19: 257–271.

Quinn, Zoe. 2017. "What happened after GamerGate hacked me." *Time*, September 11, 2017. http://time.com/4927076/zoe-quinn-gamergate-doxxing-crash-override-excerpt/

Spanos, Georgios and Lefteris Angelis. 2016. "The impact of information security events to the stock market: A systematic literature review." *Computers & Security* 58: 216–229.

Wolak, Janis and David Finkelhor. 2016. *Sextortion: Findings from a survey of 1,631 victims*. Durham, NH: Crimes against Children Research Center.

REVENGE PORN

Revenge porn refers to sexually explicit photographs or video posted online without permission of the person depicted in the photographs or video. It does not require that the photographs or video be obtained without permission, only that they be posted without permission. For example, if an individual possessing explicit images of a partner following a breakup is not illegal; however, posting those images online without the other person's consent can be illegal.

Revenge porn (referred to in statute as "unlawful dissemination of an intimate image" or something similar) has been specifically criminalized in most states. Illinois's statute (Illinois Criminal Code § 11-23.5) illustrates the elements this crime generally has. It requires that an image be intentionally disseminated that depicts someone's genitals, anus, or (if a female) nipple. It also requires that the identity of the person depicted be determinable—either from the picture itself of from text accompanying the picture. This element is necessary because being able to identify the person in the picture is what makes the picture harassing to the person depicted. The person depicted must also be 18 years of age or older. If the person depicted is younger, the image would constitute child pornography—a more severe crime. Lastly, the picture must have been obtained with the understanding that the picture was to be kept private, but then be disseminated without the consent of the person depicted.

In states that do not have specific revenge porn statutes, victims are not without recourse. States will generally have statutes that make harassment a crime. Inasmuch as the dissemination of revenge porn does harass the victim, a person could be charged with this crime in a state without a specific revenge porn statute.

Social media sites also have policies in place prohibiting the posting of revenge porn (Facebook, 2018; Reddit, 2018; Twitter, 2018). Facebook and Instagram have taken an interesting approach to prevent revenge porn. Victims of revenge porn, or those who believe they will be the victims of revenge porn, can send the photographs in question to Facebook or Instagram, which can then block copies of those photographs from showing up on their platforms (Instagram, 2018; Solon, 2017). It does require the victim to provide sexually explicit photographs of themselves to a large corporation. At least one employee will have to look at the picture in order to produce a digital image hash—a unique code that is generated for the image—that can be used to detect when that same image is posted to Facebook (Romano, 2018). Facebook does delete the image after the digital image hash is created and only stores the hash. Despite this, Facebook's system of dealing with revenge porn has been criticized for—among other things—potentially revictimizing victims of revenge porn (Romano, 2018).

Sextortion is another crime that is similar to revenge porn. Sextortion is the act of threatening to release sexual content of the victim (photographs, video, etc.) unless the victim agrees to provide something to the perpetrator (e.g., money, sex). In other words, sextortion involves someone who is generally in possession of materials that would be considered revenge porn, and instead of releasing those images outright to harass the victim, the threat of releasing those images is used to extort something from the victim. Where sextortion is a specific subcategory of extortion, it will generally already be a prosecutable offense under a state's extortion statute.

Sextortion is a growing concern. Getting a handle on exactly how many people fall victim to sextortion can be difficult. In the United Kingdom, over 1,300 incidents of sextortion were reported in 2017 (see National Crime Agency, 2018). The National Crime Agency notes it is likely that number is much higher, as many victims do not report when they are the victim of sextortion. One study found that only 16 percent of sextortion victims reported the incident to law enforcement (Wolak and Finkelhor, 2016). That same study found that only a third of victims told anyone they were the victim of sextortion.

Sextortion can even reach the famous. One case that made headlines was that of then-Golden State Warriors coach Mark Jackson. Jackson had carried on an affair with a former stripper. She and an accomplice later used pictures that had been taken of Jackson and her to extort money from him. The first time he was approached, he did provide money. After they approached him a second time for more money, he contacted the FBI (Lee, 2012).

The harm of sextortion can extend beyond just monetary loss. Victims may feel the need to seek medical or mental health professional or, in some instances, feel the need to move because they do not feel safe where they currently live (Wolak and Finkelhor, 2016). In a handful of cases, it may even drive the victim to commit suicide (National Crime Agency, 2018).

See also: Child Pornography; Cyberbullying; Sexting

Further Reading

Facebook. 2018. "Not without my consent." Facebook. https://fbnewsroomus.files.wordpress.com/2017/03/not-without-my-consent.pdf

Instagram. 2018. "What should I do if someone shares an intimate photo of me without my permission?" Instagram. https://help.instagram.com/1769410010008691?helpref=search&sr=1&query=revenge%20porn

Lee, Henry K. 2012. "Woman, man charged in Mark Jackson extortion case." *San Francisco Chronicle*, June 29, 2012. https://www.sfgate.com/warriors/article/Woman-man-charged-in-Mark-Jackson-extortion-case-3672018.php

National Crime Agency. 2018. "Record numbers of UK men fall victim to sextortion gangs." http://www.nationalcrimeagency.gov.uk/news/1360-record-numbers-of-uk-men-fall-victim-to-sextortion-gangs

Reddit. 2018. "Do not post involuntary pornography." https://www.reddithelp.com/en/categories/rules-reporting/account-and-community-restrictions/do-not-post-involuntary-pornography

Romano, Aja. 2018. "Facebook's plan to stop revenge porn may be even creepier than revenge porn." *Vox*, May 24, 2018. https://www.vox.com/2018/5/23/17382024/facebook-revenge-porn-prevention

Solon, Olivia. 2017. "Facebook asks users for nude photos in project to combat 'revenge porn.'" *The Guardian*, November 7, 2017. https://www.theguardian.com/technology/2017/nov/07/facebook-revenge-porn-nude-photos

Twitter. 2018. "About intimate media on Twitter." https://help.twitter.com/en/rules-and-policies/intimate-media

Wolak, Janis, and David Finkelhor. 2016. *Sextortion: Findings from a survey of 1,631 victims*. Durham, NH: Crimes against Children Research Center.

ROOTKIT

A rootkit is malware that is able to disguise its existence on an infected computer. It does so by hiding existence of various elements—files, processes, network connections, and so on—from other programs on the computer or from the computer's operating system (Goncharov, 2012). Rootkits generally try to hide these elements from antivirus software and similar security tools (Kaspersky, 2013). By doing so, a rootkit can not only avoid detection but can also avoid being removed from the infected computer.

A rootkit itself conceals the presence of malware. The payload of the rootkit can vary. Additional malware that may be included as a payload include keystroke monitors, spyware and bots. Rootkits commonly allow a cybercriminal to surreptitiously access the infected computer (Kaspersky, 2013).

There are two general categories of rootkits: rootkits that operate at the application (user) level and rootkits that operate at the kernel level (Goncharov, 2012; Kaspersky, 2013). Application-level rootkits tend to be more common. These rootkits operate by modifying applications (software) on a computer. As long as the operating system of a computer has not been infected by a rootkit, the operating system may be able to detect a rootkit operating at the application level (Shakarian et al., 2013). Accordingly, cybercriminals may attempt to use a rootkit that can affect the operating system of a computer, namely a kernel-level rootkit. A kernel is the part of a computer's operating system that communicates with the computer's hardware. The kernel manages aspects of the operating system that are necessary for it to function properly, such as data storage and memory (Santana, 2017). A kernel-level rootkit gives a cybercriminal more control over the functions of a computer. Because a kernel-level rootkit can modify the operating system of a computer and not just a single application on the computer, it is also better able to avoid detection and removal (Shakarian et al., 2013). Kernel-level rootkits are generally more complex pieces of malware and are thus less common than application-level rootkits (Kaspersky, 2013). However, where these are available via black markets online, they may not be as rare as they once were (Goncharov, 2012; Shakarian et al., 2013). For a computer infected with a kernel-level rootkit, it may be necessary to reinstall the operating system on the computer to get rid of it (Kaspersky, 2013).

Another type of rootkit that is not as common as the rootkits mentioned above is a bootkit. As noted above, it is sometimes necessary to reinstall the operating system on the computer to get rid of it. A bootkit infects and modifies a computer's boot loader. A boot loader is the program on a computer that loads the operating system. Accordingly, it runs before an operating system runs. Thus, if a bootkit is installed on a computer, reinstalling the operating system may not get rid of it (Goncharov, 2012; Kaspersky, 2013).

See also: Bots and Botnets; Keystroke Monitoring; Malware; Payload; Spyware

Further Reading

Goncharov, Max. 2012. "Russian underground 101." Trend Micro Incorporated. https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

Kaspersky. 2013. "What is a rootkit and how to remove it." Kaspersky, March 28, 2013. https://usa.kaspersky.com/blog/rootkit/1508/

Santana, Mario. 2017. "Eliminating the security weakness of Linux and UNIX operating systems." In *Computer and information security handbook*, 3rd Edition, edited by John R. Vacca. Cambridge, MA: Elsevier.

Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. 2013. *Introduction to cyber warfare: A multidisciplinary approach*. Waltham, MA: Elsevier.

RUSSIA

Cybercrime is an issue in Russia just as it is in the United States. Research in 2017 indicated that over one-third of Russians had been the victims of a cybercrime (*Moscow Times*, 2017). The policies and practices of the Russian government with regard to cybercrime enforcement, however, would appear to encourage cybercriminals to commit cybercrimes against foreign targets rather than domestic targets. Evidence suggests that Russia tends to not concern itself with the apprehension of cybercriminals who attack foreign targets, whereas those who attack domestic targets risk apprehension (Maurer, 2018). It would appear that Russian cybercriminals are aware of this. For example, in 2018, 36 defendants from around the world were indicted in the United States for their roles in the Infraud Organization—a cybercrime organization that trafficked in personally identifying information of victims, financial account information of victims, and malware (United States Department of Justice, 2018a). The Infraud Organization website was hosted in Russia. In 2011, the website's founder prohibited trafficking of information belonging to Russian victims. It appears that Russia did not assist the United States in bringing down the Infraud Organization (Carlin and Newman, 2018). Additionally, there is evidence that some Russian-made malware is designed to avoid attacking computers of Russian residents, and some websites that install spyware as a paid service refuse to install it on Russian computers (Maurer, 2018).

Russia has a fairly established cybercrime black market. In 2006, the Russian Business Network (RBN) was established. The RBN was an ISP based in Russia. The RBN initially hosted legitimate websites. However, it soon hosted almost exclusively (if not entirely exclusively) websites engaged in cybercrime. It provided bulletproof hosting—hosting that will continue even if the website in question is involved in illegal activities. At the time, it was estimated that the RBN was responsible for 60 percent of all cybercrime worldwide. The RBN went offline in 2007 (Warren, 2007). The cybercrime black market in Russia, however, still exists. The current cybercrime black market operates much like a legal market and caters to numerous cybercrime needs (Goncharov, 2012; Steadman, 2012). The goods and services available for purchase in that market include DDoS attacks, spamming, and rootkits. Prices vary depending on the good or service sought. A rootkit, for example, can cost around $500. Services vary depending on the needs of the customer. Spam services can be relatively inexpensive. Some spam services will distribute one million e-mails for as little as $10. DDoS attacks can be inexpensive as well. You can purchase the shutdown of a website for a full day for as low as $30. If you wish to shut down a website for a longer period of time, it can get more expensive. To shut a site down for a month would cost about $1,200 (Goncharov, 2012). The relatively low cost of many cybercrime goods and services enables more people to engage in cybercrime (Barbaschow, 2017).

Russia itself has carried out numerous cyberattacks against foreign entities. From 2006 to early 2019, Russia carried out just under 100 cyberattacks against foreign entities—second only to China. The countries attacked include the United States, Germany, Estonia, Georgia, and Ukraine (Center for Strategic and International Studies, 2019). There are two methods by which Russia tends to carry out state-sanctioned cyberattacks against foreign entities. First, there are instances when state officials carry out the attack. This can be seen in a U.S. indictment against members of the Russian GRU. This case stemmed from an antidoping investigation into Russian athletes that arose around the Sochi Winter Olympics in 2014. That investigation found there was a state-sponsored system in place in Russia to circumvent testing for banned substances in their athletes.

From 2014 to 2018, seven officers in the GRU hacked into the networks of several foreign entities for the purpose of gathering information that could be used to spread disinformation about the antidoping investigation. The goal was to discredit the investigation (United States Department of Justice, 2018b). In another instance of state-sponsored hacking, three of the officers involved in the cyberattacks above were also involved in the hack of Democratic National Committee (DNC) e-mails in the United States prior to the 2016 presidential election in the United States (*U.S. News*, 2018). The other tactic Russia uses to perpetrate state-sponsored cyberattacks is the use of existing cybercrime organizations. In those instances, Russia will use nonstate actors to carry out cyberattacks on behalf of the Russian government. There are advantages to this system. It creates ambiguity when authorities attempt to track down the offender. Investigators may be unable to clearly tie the attack of a private actor working for Russia back to Russia itself. This ambiguity provided Russia with plausible deniability with regard to these cyberattacks (Cybereason Intel Team, 2017).

In some instances, those carrying out cyberattacks for Russia may be compelled to do so. This can be seen in the Yahoo data breach in 2014. In that case, Russian operatives hacked into Yahoo and stole the personal information of over 500 million customers. In that case, Russian operatives worked with two cybercriminals: Alexsey Alexseyevich Belan and Karim Baratov. It appears Belan agreed to work with Russian officials to avoid arrest and extradition by those officials on prior cybercrime charges out of the United States and Europe. Oleg Gordievsky, the former head of the KGB's London office, indicated in 1998 that such arrangements are made by the Russian government with apprehended cybercriminals. For other cybercriminals, they may agree to cooperate with the Russian government for economic benefit. In the Yahoo data breach, Baratov appears to have cooperated for this purpose (Maurer, 2018). While there are advantages to outsourcing cyberattacks, there is evidence to suggest that Russia's ability to control the private cybercriminal groups they use is lessening. The incentives that can be offered to cybercriminals by Russia decrease as cybercrime becomes more global and incentives from other sources increase (Cybereason Intel Team, 2017).

One type of cyberattack that Russia has used with some frequency is misinformation campaigns. As was mentioned above, Russia engage in such an attack to discredit the investigation into Russia's athlete doping program. Perhaps the best-known misinformation campaign perpetrated by Russia involved the 2016 presidential election in the United States. Leading up to the presidential election in 2016, Russia engaged in misinformation campaign with the goal of creating discord within the political system in the United States and influencing the 2016 presidential election. This was done through the IRA. Members of the IRA used fabricated social media accounts—on sites like Facebook, Instagram, and Twitter—through which they claimed they were activists in the United States. These accounts sometimes falsely claimed affiliation with actual political organizations within the United States, such as the Tennessee GOP. Additionally, social media advertisements were also purchased by the IRA under the names of persons and other entities in the United States. This misinformation campaign was accompanied by cyberattacks on the computers of presidential candidate Hilary Clinton, wherein information was stolen and publicly released (Mueller, 2019). The United States is not the only country that has been attacked by Russia with a misinformation campaign. In 2017, Sweden was also target by Russia. It appears that Russia spread false documents and other misinformation with the intent of weakening public support for policies in Sweden (Center for Strategic and International Studies, 2019).

Russia has also been the target of cyberattacks from other countries. Russia and Russian industries have been targeted by China, North Korea, and countries in the Middle East. The United States also announced in 2018 that it targeted Russian cyberoperatives it feared might try to interfere in the 2018 election in the United States. The United States stated this was a deterrence measure (Center for Strategic and International Studies, 2019).

See also: Distributed Denial-of-Service Attack (DDoS); International Issues; Malware; Political Uses; Rootkit; Russian Business Network; Social Media; Spam; State Actor; U.S. Presidential Election Interference, 2016

Further Reading

Barbaschow, Asha. 2017. “Low-cost tools making cybercrime more accessible: SecureWorks.” ZDNet, September 19, 2017. https://www.zdnet.com/article/low-cost-tools-making-cybercrime-more-accessible-secureworks/

Carlin, John, and David Newman. 2018. “Russian cybercrime bust paints ‘striking picture’ of ‘dark-web’ operation, former FBI official says.” *CNBC*, February 22, 2018. https://www.cnbc.com/2018/02/22/russian-cybercrime-bust-and-how-fight-the-hackers-commentary.html

Center for Strategic and International Studies. 2019. “Significant cyber incidents.” https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

Cybereason Intel Team. 2017. “Russia and nation-state hacking tactics: A report from cybereason intelligence group.” Cybereason, June 5, 2017. https://www.cybereason.com/blog/blog-russia-nation-state-hacking-the-countrys-dedicated-policy-of-strategic-ambiguity

Goncharov, Max. 2012. “Russian underground 101.” Trend Micro Incorporated. https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

“The latest: Russian envoy rejects reports of cybercrimes.” *U.S. News*, October 4, 2018. https://www.usnews.com/news/world/articles/2018-10-04/the-latest-russian-envoy-rejects-reports-of-cybercrimes

Maurer, Tim. 2018. “Why the Russian government turns a blind eye to cybercriminals.” *Slate*, February 2, 2018. https://slate.com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals.html

Mueller, Robert S. 2019. “Report on the investigation into Russian interference in the 2016 presidential election.” Volume 1. United States Department of Justice. https://www.justice.gov/storage/report.pdf

Steadman, Ian. 2012. “The Russian underground economy has democratised cybercrime.” *Wired*, November 2, 2012. https://www.wired.co.uk/article/russian-cybercrime

“Third of Russians are victims of cyber-crime—Poll.” *The Moscow Times*, January 11, 2017. https://www.themoscowtimes.com/2017/01/11/third-of-russians-are-victims-of-cyber-crime-poll-a56782

United States Department of Justice. 2018a. “Thirty-six defendants indicted for alleged roles in transnational criminal organization responsible for more than $530 million in losses from cybercrimes.” https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible

United States Department of Justice. 2018b. "U.S. charges Russian GRU officers with international hacking and related influence and disinformation operations." https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

Warren, Peter. 2007. "Hunt for Russia's web criminals." *The Guardian*, November 15, 2007. https://www.theguardian.com/technology/2007/nov/15/news.crime

RUSSIAN BUSINESS NETWORK

The Russian Business Network (RBN) was an ISP based in Russia. It was established in 2006. When the RBN started, it initially hosted many legitimate websites. However, it soon began hosting websites that were engaged in cybercrime. A study scanned all the internet addresses registered to the RBN at one point and found that every single website was involved in some criminal enterprise. While it was in operation, it was estimated that the RBN was responsible for 60 percent of all cybercrime worldwide (Warren, 2007).

Getting the RBN to host a website was not straightforward. The RBN did not have a homepage through which the administrators could be contacted. Contact with administrators had to be accomplished by sending them an instant message or through specified online forums that were Russian language–based. Those wishing to have their website hosted through RBN would also have to prove to the administrators that they were neither law enforcement officers nor working with law enforcement. This generally required the applicant to demonstrate they were involved in the theft of financial and personally identifying information of victims (Krebs, 2007).

One of the draws of the RBN for cybercriminals was the bulletproof hosting it provided. Bulletproof hosting is website hosting that continues despite law enforcement efforts to shut the website down or complaints made to RBN. This permitted cybercriminals to function without interruption. Bulletproof hosting came at a cost. The RBN charged $600 a month to have a website hosted—approximately 10 times as much as website hosting through a traditional ISP would have cost at the time (Krebs, 2007). Exactly how the RBN was able to provide such services without being shut down by Russian law enforcement is not known. However, there are some factors that likely contribute to their ability to provide the service. Those operating on the RBN tended to not target Russian citizens when carrying out cybercrimes, thus avoiding local attention. There were allegations that the RBN had ties to the Russian government. The creator of the RBN—known online as Flyman—is believed to be the nephew of a prominent Russian politician (Warren, 2007). There were also allegations that bribery of government officials may have taken place (Krebs, 2007).

Prosecuting the RBN proved difficult when it was in operation. As an ISP, it was not technically involved in cybercrime. It simply hosted websites that were engaged in cybercrime (Krebs, 2007). The RBN itself essentially made this argument when defending against claims that it was responsible for a substantial amount of cybercrime around the world. The RBN claimed that no more cybercrime happened on its network than any other ISP (Singel, 2007). It also claimed that it addressed complaints of criminal activity taking place on its network promptly. There is some indication that the RBN would take down websites engaged in criminal activity and technically comply with efforts to remove criminal content from its network, but those websites would be back online the next day (Singel, 2007).

The RBN was fairly short-lived. It ceased operations in 2007. In November of that year, the RBN attempted to move its operation from servers in St. Petersburg, Russia, to servers in China. This occurred as the RBN was attracting attention from various cybersecurity groups who were trying to track down those behind the RBN. The attempted move was unsuccessful, and the RBN essentially disappeared at that point (Warren, 2007). However, there is evidence to suggest that members of the RBN are still engaged in the same activities as they were when the RBN was still operating, albeit under different names. These activities include offering bulletproof hosting for cybercriminal operations (Leyden, 2017).

See also: Personally Identifying Information; Russia

Further Reading

Krebs, Brian. 2007. "Shadowy Russian firm seen as conduit for cybercrime." *The Washington Post*, October 13, 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html

Leyden, John. 2017. "Bulletproof hosts stay online by operating out of disputed backwaters." *The Register*, October 5, 2017. https://www.theregister.co.uk/2017/10/05/bulletproof_hosting/

Singel, Ryan. 2007. "Russian hosting firm denies criminal ties, says it may sue blacklister." *Wired*, October 15, 2007. https://www.wired.com/2007/10/russian-hosting-firm-denies-criminal-ties-says-it-may-sue-blacklister/

Warren, Peter. 2007. "Hunt for Russia's web criminals." *The Guardian*, November 15, 2007. https://www.theguardian.com/technology/2007/nov/15/news.crime

S

SCAVENGING

Generally speaking, scavenging is the practice of going through something that has been discarded for the purpose of trying to find something valuable. This includes finding items in the trash as well as animals finding edible flesh on the carcass of a dead animal. In the cybercrime context, scavenging has the same meaning. However, the valuable item being looked for with cybercrime scavenging is generally the personally identifying information of others. If a cybercriminal is able to find such information, it can then be used by them to commit various crimes, such as theft in general, identity theft, and other financial crimes. Cybercriminals might also scavenge manuals that describe how an organization's computer network operates (Chabinsky, 2010). This information can assist a cybercriminal in exploiting that organization's computer network to commit further cybercrimes.

Scavenging generally takes one of two forms. First, cybercriminals may engage in physical scavenging, going through garbage to obtain personally identifying information (Parker, 1989). This could be done anywhere. If a cybercriminal were to go through the garbage at someone's residence, they could potentially find personally identifying information, such as a victim's name and address from discarded mail or even financial information such as a bank account number if the victim threw away a bank statement. However, for a cybercriminal seeking to obtain personally identifying information that will enable them to commit a cybercrime, there may be more fruitful options. The garbage cans of banks and other financial institutions may be more likely to contain documents with financial information on them, and the number of victims whose data is on those documents is likely to be greater than in the garbage can of a residence.

Another method of scavenging is scavenging for residual data on a computer or other electronic device (Parker, 1989). At a basic level, this could include gathering the login credentials of a victim that used them to log into a public computer and forgot to log out before leaving. If an electronic device is thrown away and the owner did not properly remove the data contained on it before doing so, a cybercriminal could scavenge that data as well. Digital scavenging can at times be more complex than this. There are methods that can be used to obtain residual data from an electronic device even after a user attempts to delete that data from the device. For example, deleted data is often not completely deleted from an electronic device until it is overwritten by something new (Sandell, 2012). With the proper tools, a cybercriminal could access that data and scavenge the needed information from it.

Cybercriminals are not the only ones who use digital scavenging techniques. Cybercrime investigators can use those techniques to solve crimes as well. This occurred in 1987 during the investigation of the Iran-Contra affair. As part of the investigation into that incident, it was discovered that Oliver North—a member of the United States National Security Council at the time—had deleted e-mails relevant to the investigation. However, his attempts to delete the e-mails had only removed them from the directory of messages. The contents of those e-mails continued to exist and were discovered by investigators (Parker, 1989). These techniques are still used by investigators. In 2010, federal regional computer forensic labs (RCFLs) in the United States reviewed over 3,000 terabytes of data as part of investigative efforts (Sandell, 2012).

See also: Financial Crimes; Identity Theft; Personally Identifying Information

Further Reading

Chabinsky, Steven R. 2010. "The cyber threat: Who's doing what to whom?" Federal Bureau of Investigation, March 23, 2010. https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom

Parker, Donn B. 1989. *Computer crime: Criminal justice resource manual*. United States Department of Justice. https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf

Sandell, Clayton. 2012. "Digital Detectives Dig Through Data Deluge." *ABC News*, January 30, 2012. https://abcnews.go.com/Technology/fbis-digitial-detectives-recover-deleted/story?id=15470999

SECRET SERVICE

The Secret Service is a federal law enforcement agency in the United States. It was founded in 1865. Its initial mission—which still pertains today—was to investigate crimes relating to the U.S. financial system (United States Secret Service, 2017). The Secret Service was additionally tasked with investigating computer crimes in 1984. Its authority to do so was broadened in 2001 under the PATRIOT Act (House Committee on Oversight and Government Reform, 2015).

Increasingly, the role of the Secret Service to investigate financial crimes and its role to investigate cybercrimes overlap. As technology has advanced, financial systems have become increasingly digitized and rely this technology to operate. While this has permitted financial transactions to take place more expeditiously, it has also exposed the financial sector to the risks associated with operating in a cyberenvironment (United States Secret Service, 2017). This would include hacking, social engineering, phishing, and other cyberattacks. The efforts of the Secret Service prevent a significant amount of loss in the financial sector. In 2017, it prevented over $3 billion of loss (United States Secret Service, 2017).

The Secret Service has been involved in several large investigations. In 2006, the Secret Service, along with the Federal Bureau of Investigation (FBI), investigated CardersMarket—the largest English-speaking online criminal marketplace at the time. The site sold the personally identifying information of victims to cybercriminals. That information was obtained by CardersMarket in part by stealing it from other websites that already had the information for sale (Poulson, 2009). Max Vision—the site's founder—was ultimately sentenced to 13 years in prison and ordered to pay $27.5 million in restitution (Poulsen, 2010).

The Secret Service has worked with law enforcement in other countries when investigating cybercrime. In 2018, the Secret Service and other U.S. law enforcement agencies worked with law enforcement in Canada, Indonesia, Malaysia, Mauritius, Nigeria, and Poland in Operation Wire Wire. Operation Wire Wire investigated hackers involved in business e-mail compromise schemes—attacks where corporate e-mail accounts are compromised in order to fraudulently wire money from those businesses to cybercriminals. The operation resulted in the arrest of 74 people internationally, 42 of whom were arrested in the United States (United States Department of Justice, 2018).

Another international investigation was conducted by the Secret Service in 2019. That year, the Secret Service arrested individuals—primarily from Romania—for defrauding victims in the United States through the use of fictitious auctions on eBay and other sites. The cybercriminals would advertise items for sale that did not exist. They would then accept the money from the victims and never deliver the goods (United States Department of Justice, 2019).

Another cybercrime threat faced by the financial system is cryptocurrency. Because cryptocurrencies offer some level on anonymity to the user, they are often used by cybercriminals to launder money. Indeed, the cybercriminals in the auction fraud case mentioned above used cryptocurrency to launder the fraudulently obtained proceeds of the auctions to coconspirators in Romania (United States Department of Justice, 2019). The Secret Service has been able to essentially shut down two cryptocurrencies through their efforts—e-Gold and Liberty Reserve (United States Secret Service, 2017). The Secret Service has asked the U.S. Congress for legislative assistance in regard to cryptocurrency, advocating additional regulations that would allow law enforcement to combat the anonymity afforded by many cryptocurrencies (Stanley, 2018).

In addition to investigating cybercrimes, the Secret Service operates the National Computer Forensic Institute. The Institute provides cybercrime training to law enforcement and court personnel (House Committee on Oversight and Government Reform, 2015).

One of the key responsibilities of the Secret Service is the protection of the president of the United States. This responsibility was informally undertaken at first. In 1894, President Grover Cleveland asked for the Secret Service to provide protection for him. Following the assassination of President William McKinley in 1901, the U.S. Congress formally gave the responsibility of presidential protection to the Secret Service and provided it funding to do so in 1906. Since that time, the scope of protection the Secret Service is to provide has extended to the vice president, former presidents, major presidential and vice presidential candidates, and the immediate families of those persons. A 2015 governmental report suggested that the investigative roles of the Secret Service were cutting into its ability to provide adequate protection to the president and others it was tasked with protecting

(House Committee on Oversight and Government Reform, 2015). It suggested that the Secret Service shed—at least in part—its cybercrime and other investigative responsibilities to have the ability to focus on its protective mission. The report noted the potential overlap in responsibilities in cybercrime investigations that can happen at the federal level. Numerous federal agencies are involved in cybercrime investigations in addition to the Secret Service. These include the FBI; Immigration and Customs Enforcement (ICE); the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF); the Federal Trade Commission (FTC); the Securities and Exchange Commission (SEC); and Postal Inspection Service. The report notes that if the cybercrime investigative functions of some of these agencies were consolidated, it would be a more efficient use of resources.

See also: Cryptocurrency; Federal Bureau of Investigation; Financial Crimes; Hacker and Hacking; Immigration and Customs Enforcement; Money Laundering; Phishing; Social Engineering

Further Reading

House Committee on Oversight and Government Reform. 2015. "United States Secret Service: An agency in crisis." United States House of Representatives, December 9, 2015. https://docs.house.gov/meetings/GO/GO00/20151209/104284/HRPT-114-1.pdf

Poulson, Kevin. 2009. "The decade's 10 most dastardly cybercrimes." *Wired*, December 31, 2009. https://www.wired.com/2009/12/ye-cybercrimes/

Poulson, Kevin. 2010. "Record 13-year sentence for hacker max vision." *Wired*, February 12, 2010. https://www.wired.com/2010/02/max-vision-sentencing/

Stanley, Aaron. 2018. "U.S. Secret Service: Action needed to address anonymous cryptocurrencies." *Forbes*, June 20, 2018. https://www.forbes.com/sites/astanley/2018/06/20/u-s-secret-service-action-needed-to-address-anonymous-cryptocurrencies/#63381b073ca1

United States Department of Justice. 2018. "74 arrested in coordinated international enforcement operation targeting hundreds of individuals in business email compromise schemes." June 11, 2018. https://www.justice.gov/opa/pr/74-arrested-coordinated-international-enforcement-operation-targeting-hundreds-individuals

United States Department of Justice. 2019. "United States and international law enforcement dismantle online organized crime ring operating out of Romania that victimized thousands of U.S. residents." February 7, 2019. https://www.justice.gov/opa/pr/united-states-and-international-law-enforcement-dismantle-online-organized-crime-ring

United States Secret Service. 2017. "Office of investigations: Priorities and roadmap." https://www.secretservice.gov/data/investigation/INV_Priorities_and_Roadmap_2017_Final_U.pdf

SEXTING

Sexting is the act of electronically sending sexually explicit messages or photographs to another person. For adults (those over the age of 18), the practice is not generally of legal concern. For minors (those under the age of 18), there are potential criminal ramifications in the United States. The concern is with sexually explicit photographs of minors. Possessing, taking, or distributing such a photograph would likely be a crime under a state or federal child pornography statute.

There are situations where one minor will send another minor a sexually explicit photograph of himself or herself. One study indicates 4 percent of teens with a cell phone have sent a sexually suggestive nude or nearly nude photograph of themselves and that 15 percent of teens with a cell phone have received such a photograph (Lenhart, 2009). Another study indicates 2.5 percent of teens have sent or appeared in a nude or nearly nude photograph and that 7.1 percent had received such a photograph (Mitchell et al., 2012). Those numbers drop when considering photographs that did not merely contain nudity but are also of a sexually explicit nature. One percent of teens indicated they had appeared in or sent a sexually explicit photograph, and 5.9 percent indicated they had received such a photograph (Mitchell et al., 2012).

One sexting case in Washington resulted in three minors being charged. In 2010, the photograph of a naked 14-year-old girl was circulated among students at the girl's middle school as well as at other schools. The picture was initially sent to her boyfriend, but after the couple broke up, her boyfriend sent the picture to another girl. That girl and one other girl widely disseminated the picture from there. The boyfriend and the two girls were charged with distribution of child pornography, as no specific sexting statute was in place as the time (Pawloski, 2010). It appears this was done maliciously and thus fits the profile of revenge porn. One of the girls who disseminated the photograph sent it with the caption, "Ho Alert! If you think this girl is a whore, then text this to all your friends." The three teens ultimately pled guilty to misdemeanor charges of telephone harassment (Hoffman, 2011).

Given the prevalence of sexting among minors, several states have enacted laws to address the situation. Twenty-two states currently have laws that address sexting. The majority of these statutes treat the offense as a misdemeanor. New Mexico's sexting statute is unique in that minor-to-minor sexting is exempt from criminal liability. For those states that have not passed specific sexting laws (and even among those that have), child pornography laws may still apply to minors who send or receive sexually explicit pictures, as it did in the Washington case above.

While sexting between two consenting adults is not generally going to be criminal, sexting between an adult and a minor would be. This behavior would not fall under a state sexting statute, as those statutes are generally designed to regulate the sending of sexually explicit pictures between minors. Rather, an adult engaging in such behavior could be charged with child pornography and similar offenses. One case involving the sending of sexually explicit images and messages between an adult and a minor is the case of Anthony Weiner, a former U.S. congressman from New York. In that case, Weiner solicited a girl whom he knew to be 15 years old to send images of herself to him in sexually suggestive positions. Weiner pled guilty to transferring obscene material to a minor for his sexually explicit communications. He was sentenced to 21 months in prison (Herbst, 2017).

While sexting can have consequences in the criminal justice system, there can be other consequences from sexting. As noted above, what might start as a consensual sharing of sexually explicit pictures between minors can sometimes devolve into a situation when those pictures are shared as revenge porn. This can have a significant emotional impact on the person in the pictures. There are at least two instances—one in 2008 and the other in 2009—where this has resulted in the minor depicted in the pictures committing suicide (see Celizic, 2009; Kaye, 2010).

See also: Child Pornography; Revenge Porn

Further Reading

Celizic, Mike. 2009. "Her teen committed suicide over 'sexting.'" *Today*, March 6, 2009. https://www.today.com/parents/her-teen-committed-suicide-over-sexting-2D80555048

Herbst, Diane. 2017. "Anthony Weiner gets federal prison for sexting teenager—In case that shook presidential election." *People*, September 25, 2017. https://people.com/crime/anthony-weiner-sentenced-sexting-teen-girl/

Hinduja, Sameer, and Justin W. Patchin. 2015. "State sexting laws." Cyberbullying Research Center. https://cyberbullying.org/state-sexting-laws.pdf

Hoffman, Jan. 2011. "A girl's nude photo, and altered lives." *New York Times*, March 26, 2011. https://www.nytimes.com/2011/03/27/us/27sexting.html

Kaye, Randi. 2010. "How a cell phone picture led to girl's suicide." CNN, October 7, 2010. http://www.cnn.com/2010/LIVING/10/07/hope.witsells.story/index.html

Lenhart, Amanda. 2009. "How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging." *Pew Internet & American Life Project*. https://www.pewresearch.org/internet/2009/12/15/teens-and-sexting/

Mitchell, Kimberly J., David Finkelhor, Lisa M. Jones, and Janis Wolak. 2012. "Prevalence and Characteristics of Youth Sexting: A National Study." *Pediatrics*, Vol. 129, No. 1, pp. 13–20. https://doi.org/10.1542/peds.2011-1730

Pawloski, Jeremy. 2010. "Third Lacey student charged in nude-photo 'sexting' case." *The Olympian*, January 29, 2010. https://www.theolympian.com/news/local/article25247320.html

SILK ROAD

Silk Road was an online marketplace founded in 2011 by Ross Ulbricht, who went by the online name of Dread Pirate Roberts. Ulbricht had initially referred to the project as Underground Brokers before settling on the name Silk Road (Bearman et al., 2015a). The term Silk Road comes from the ancient trade routes of the same name. The site operated on the dark web and was notorious for facilitating drug sales. In the short time that Silk Road was in operation, it managed to amass over a million customers worldwide and over $1 billion in sales (Bearman et al., 2015a).

For Ulbricht and many of the site's users, Silk Road was about more than just selling drugs. Ulbricht espoused libertarian ideology. The idea behind creating Silk Road was providing a marketplace were users could buy and sell goods that Ulbricht believed the government had no business regulating—and could do so without fear of getting in trouble for it. This, he believed, provided true freedom. Consistent with this ideology, Silk Road did not permit any and all criminal goods and services to be trafficked on the site. Things like drugs were permitted to be bought and sold because the use of drugs was not seen to infringe on the freedom of anyone else. Measures to prevent potential drug sales to children were not implemented, as doing so was seen as a restriction on the freedom of those children. Other items, such as child pornography and stolen goods, were prohibited because the existence of those items did infringe of the freedom of others (Bearman et al., 2015a, 2015b).

To help assure the anonymity of purchases made through Silk Road, those purchases were made with Bitcoin. The site had a Bitcoin escrow system in place whereby Bitcoins were held until transactions were complete—a measure implemented to protect against fraudulent transactions on the site (Bearman et al., 2015a). Though this did aid with anonymity of purchases, the business did have to worry about the fluctuations in value of Bitcoin and other issues relating to the cryptocurrency. For example, Mt. Gox—the largest Bitcoin exchange at the time—had millions of dollars seized from it as part of a government investigation, and Silk Road had accounts with Mt. Gox (Bearman et al., 2015b).

Silk Road eventually drew the attention of law enforcement. Several federal agencies worked on the investigation into Silk Road, which was dubbed Operation Marco Polo (after the famous explorer who traveled the ancient Silk Road). Through the use of informants, undercover infiltration of the organization, and technology, in 2013, authorities were able to apprehend Ulbricht, shut down Silk Road, and seize the Bitcoin in Silk Road's escrow account (Bearman et al., 2015a, 2015b). In addition to the arrests made as part of that operation, several other users of the site have been arrested. It has been estimated that as of 2015, over 130 users of the site had been arrested (Cox, 2015). One study found that Bitcoin transactions can be exploited to determine the identity of the person behind the transaction, and this can then be used to link people to the use of sites like Silk Road (Jawaheri et al., 2018).

Although authorities shut down Silk Road in 2013, it was reopened shortly thereafter, as Silk Road 2.0. It was short-lived, lasting only a year. Authorities shut down Silk Road 2.0 in 2014 as part of Operation Onymous—a collaborative investigation of online drug markets on the dark web between the FBI and Europol (Cook, 2014). Its founder, Thomas White, was arrested as part of that investigation by law enforcement in the United Kingdom. White originally went by the online name of StExo when working with the first iteration of Silk Road. When the second version of Silk Road started, White adopted a variation of the moniker used by his predecessor: Dread Pirate Roberts 2. White pleaded guilty to drug trafficking, money laundering, and making indecent images of children. In 2019, he was sentenced to just over five years in prison (Cox, 2019).

Silk Road 3.0 opened just hours after Silk Road 2.0 was taken down, prompting some to fear the new version of the site was being run by the government as a trap (Nelson, 2014). As of early 2019, there appears to be a Silk Road 3.1 in operation.

See also: Bitcoin; Cryptocurrency; Dark Web; Digital Currency; Dread Pirate Roberts (Ulbricht, Ross; 1984–); Drug Trafficking; Operation Marco Polo; Tor (The Onion Router)

Further Reading

Bearman, Joshuah, Joshua Davis, and Steven Leckart. 2015a. “The rise & fall of Silk Road, part 1.” *Wired*. https://www.wired.com/2015/04/silk-road-1/

Bearman, Joshuah, Joshua Davis, and Steven Leckart. 2015b. “The rise & fall of Silk Road, part 2.” *Wired*. https://www.wired.com/2015/05/silk-road-2/

Cook, James. 2014. “FBI arrests former SpaceX employee, alleging he ran the ‘deep web’ drug marketplace Silk Road 2.0.” *Business Insider*, November 6, 2014. https://www.businessinsider.com/fbi-silk-road-seized-arrests-2014-11

Cox, Joseph. 2015. “This researcher is tallying all the arrests from dark web markets.” *Motherboard*. https://www.vice.com/en_us/article/z4m77a/this-researcher-is-tallying-arrests-from-dark-web-markets

Cox, Joseph. 2019. “Silk Road 2 founder Dread Pirate Roberts 2 caught, jailed for 5 years.” *Motherboard*, April 12, 2019. https://motherboard.vice.com/en_us/article/9kx59a/silk-road-2-founder-dread-pirate-roberts-2-caught-jailed-for-5-years

Jawaheri, Husam Al, Mashael Al Sabah, Yazan Boshmaf, and Aiman Erbad. 2018. “When a small leak sinks a great ship: Deanonymizing Tor hidden service users through Bitcoin transactions analysis.” *Arxiv*. https://arxiv.org/pdf/1801.07501.pdf

Nelson, Steven. 2014. “Silk Road 3.0 Opens for Business.” *U.S. News & World Report*, November 7, 2014. https://www.usnews.com/news/articles/2014/11/07/silk-road-30-opens-for-business

SIMULATION

Simulating cybercrime is where a fake cybercrime is carried out. Simulated cybercrimes are not generally carried out by cybercriminals. Rather, simulated cybercrimes are carried out by organizations seeking to avoid being victimized by cybercrime. Cybercrime simulations can accomplish this in one of two ways. First, simulations can be used to train employees of the organization on how to address and resist cyberattacks. Second, simulations can be used by the organization to test the vulnerability of the organization’s computer network.

Simulations are used by organizations to help train personnel how to respond to cyberattacks. Interpol provides simulation training for law enforcement (Interpol, 2019). For the financial sector, there is a training event known as Quantum Dawn that is held every other year. The Quantum Dawn simulations can be complex. In 2017, the simulation included 900 participants from 50 different organizations, including banks, regulators, and law enforcement agencies. The simulation lasted two days (Cowley, 2018). In complex simulations such as these, not only do employees receive practical training on how to respond internally to cyberattacks, but they also gain experience cooperating with other relevant agencies that will be involved should an actual cyberattack hit.

Simulations can also be used to discover vulnerabilities in an organization’s computer network. This can be done by an organization itself, or it can be outsourced to white-hat hackers—hackers who specifically hack computer networks to discover vulnerabilities of those networks. Outsourced hacking to white-hat hackers can take one of two forms. Some organizations will contract directly with a hacker or hacker group to simulate a cyberattack. Other organizations will offer what are known as a "bug bounty"—a monetary reward provided to a freelance hacker for discovering a bug in an organization's network security that was previously unknown (Bergal, 2018). For organizations simulating cyberattacks against itself, the simulations will sometimes extend beyond just testing for programming bugs. One potential weak link in cybersecurity is human beings. A common tactic used by cybercriminals to infiltrate a computer network is phishing—fraudulently eliciting personal information from personnel authorized to access the computer network in question. That personal information can be used by a cybercriminal to gain access to the computer network themselves. In one simulation, the Royal Bank of Scotland conducted a simulation whereby it launched phishing attacks against its employees. The simulation helped the bank identify employees who were susceptible to phishing attacks. The bank was then able to train those employees on phishing attacks. This reduced the success rate of phishing attacks on the bank by 78 percent (Waugh, 2019).

See also: Interpol; Phishing; Vulnerability; White-Hat Hackers

Further Reading

Bergal, Jenni. 2018. "White-hat hackers to the rescue." The Pew Charitable Trusts, May 14, 2018. https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2018/05/14/white-hat-hackers-to-the-rescue

Cowley, Stacy. 2018. "Banks adopt military-style tactics to fight cybercrime." *New York Times*, May 20, 2018. https://www.nytimes.com/2018/05/20/business/banks-cyber-security-military.html

Interpol. 2019. "Cybercrime training for police." https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-training-for-police

Waugh, Rob. 2019. "Why cybersecurity training is important for your business." *The Telegraph*, June 10, 2019. https://www.telegraph.co.uk/business/ready-and-enabled/security/cybersecurity-training/

SKIMMER

A skimmer is a device placed over a legitimate payment card slot (the card slot on an ATM machine, gas pump, self-check terminal at a grocery store, etc.) that captures the information of cards put in the slot. These devices are used by cybercriminals to commit credit card fraud. Skimmers are generally small and designed to be undetectable. Some skimmers are designed to be placed over the top of the card slot, and others are designed to be inserted in the card slot (Eddy, 2019; Giorgianni, 2018). With either type of skimmer, the device is designed to read the magnetic strip on the payment card and capture the data contained therein. With many skimmers, the functionality of the machine on which they are placed is not affected (Eddy, 2019). Thus, a victim can successfully carry out a transaction (withdraw money from an ATM, pay for gas at a gas pump, etc.) without being aware that their card information has been stolen. After data is skimmed from a card, a cybercriminal needs to retrieve that data. Some skimmers store the data on a file in the device, requiring the cybercriminal to return to the machine they installed the skimmer on to retrieve it (Eddy, 2019). Other skimmers are designed to transmit the data to the cybercriminal wirelessly, allowing the cybercriminal to leave the skimmer in place indefinitely (Giorgianni, 2018). A skimmer is often accompanied by some other hardware designed to capture the PIN number that corresponds to the victim's card. Some cybercriminals will install small cameras around the ATM or other terminal to record the victim while they input their PIN number. Others may use a keypad overlay—a keypad plate that fits over the actual keypad of an ATM. The keypad overlay will record the buttons that are pushed to obtain a victim's PIN number. The keypad overlay is designed to still push the actual buttons of the ATM keypad, thus allowing a victim to complete a transaction without any indication their PIN has been stolen (Federal Deposit Insurance Corporation, 2018).

Some payment cards have changed the method in which the actual card operates, utilizing an EMV (Europay, Mastercard, and Visa) chip to conduct transactions instead of a magnetic strip. These chips provide more security than the magnetic strip (Eddy, 2019). Nonetheless, cybercriminals have created devices to intercept data from chips as well. These devices are referred to as shimmers. Due to the way EMV chips operate, shimmers are placed inside the card slot. Shimmers are able to obtain the same information that a skimmer can. The difference between chip card and a magnetic strip card is in a cybercriminal's ability to clone that card. Cybercriminals who use skimmers can use the data obtained from a magnetic strip to create a clone of the victim's card with a magnetic strip. Cybercriminals who use shimmers are able to capture card data from an EMV chip, but they are unable to create a clone of the victim's card with an EMV chip. They can, however, use the data gained from the EMV chip to create a clone of the victim's card with a magnetic strip (Eddy, 2019).

Skimming has been on the rise. In 2015, the number of ATMs compromised increased 546 percent compared to the previous year (FICO, 2016). While not as precipitous as the rise in 2015, the number of compromised ATMs and other card readers has risen in the years since then as well: 30 percent in 2016, and 8 percent in 2017 (FICO, 2017, 2018). It appears that cybercriminals tend to hit non-bank ATMs more frequently than bank-owned ATMs. In 2015 and 2016, 60 percent of the compromised ATMs were non-bank ATMs (FICO, 2016, 2017).

There are steps consumers can take to protect themselves from skimming attacks. ATMs and other payment terminals in areas that are remote and not well-lit should be avoided. If an ATM or other payment terminal looks suspicious (loose parts, mismatched parts, etc.), those should be avoided as well. When possible, conducting a financial transaction with an actual human being is preferable. If using an ATM or other payment terminal is necessary, using a mobile wallet application on a cell phone can circumvent the necessity of using a physical card. If using a physical card is necessary, covering the keypad with a hand can prevent a hidden camera (or lingering cybercriminal peeking over the victim's shoulder) from capturing the PIN number associated with the card. If a card becomes stuck in an ATM, the bank should be notified immediately as some skimmers may be designed to trap a card for a cybercriminal to retrieve later. It is recommended that credit and debit card transactions be reviewed regularly and checked for unauthorized transactions (Federal Deposit Insurance Corporation, 2018; FICO, 2018; Giorgianni, 2018).

While skimmers are generally a physical device placed on an ATM or other payment terminal to capture the card information of a victim, digital skimmers are also a possibility. A digital skimmer is malware that is installed on a legitimate website and captures a victim's credit or debit card information when it in typed in to make a purchase (Eddy, 2019). With a digital skimmer, many of the precautions mentioned above would not apply. However, there are measures that can be taken to increase security when making online purchases. One method would be to use a virtual credit card—a digital credit card number that is linked to your actual credit card. If a virtual credit card number is compromised, the number can be easily changed without having to go through the process of changing your actual credit card (Eddy, 2019).

See also: Credit Card Fraud; Malware

Further Reading

Eddy, Max. 2019. "How to spot and avoid credit card skimmers." *PCMag*, February 6, 2019. https://www.pcmag.com/article/328010/how-to-spot-and-avoid-credit-card-skimmers

Federal Deposit Insurance Corporation. 2018. "Beware of ATM, debit and credit card 'skimming' schemes." https://www.fdic.gov/consumers/consumer/news/cnwin18/cardskimming.html

FICO. 2016. "ATM compromises in U.S. jumped six-fold in 2015, FICO reports." https://www.fico.com/en/newsroom/atm-compromises-in-us-jumped-six-fold-in-2015-fico-reports-04-08-2016

FICO. 2017. "FICO reports a 70 percent rise in debit cards compromised at U.S. ATMs and merchants in 2016." https://www.fico.com/en/newsroom/fico-reports-a-70-percent-rise-in-debit-cards-compromised-at-us-atms-and-merchants-in-2016-03-29-2017

FICO. 2018. "FICO data: 10 percent more debit cards were compromised in U.S. last year." https://www.fico.com/en/newsroom/10-percent-more-debit-cards-were-compromised-in-us-last-year

Giorgianni, Anthony. 2018. "Watch your debit and credit cards: Thieves get craftier with skimmers." *Consumer Reports*, May 4, 2018. https://www.consumerreports.org/scams-fraud/thieves-get-craftier-with-skimmers-debit-cards-credit-cards/

SMART CARD

A smart card is a card (generally a plastic card that is roughly the size of a credit card) that has a microchip embedded in it. That microchip is able to both store and process data. The ability of smart cards to process and exchange data make them a more secure method of data verification than other methods, such as cards with scannable bar codes or cards with magnetic stripes (United States General Accounting Office, 2003). This increased security can help prevent fraudulent use of cards with data on them by cybercriminals.

One of the prevalent uses of smart cards is in payment cards, such as credit and debit cards. Chip-based payment cards were in use in other countries years before they were used in the United States. In France, banks first introduced chip-based payment cards in 1984, and by 1994, all French bank cards used the technology (EMVCo, 2014). Use of chip-based cards has been widespread in other European countries as well (Elkins, 2015; EMVCo, 2014). The United States did not begin widespread use of chip-based payment cards—presently referred to as EMV (Europay, MasterCard, Visa) chips—until the latter part of the 2010s. In 2014, only 0.03 percent of all payment card transactions in the United States were completed using a card with an EMV chip (EMVCo, 2014). That number increased to 41.21 percent in 2017 and 53.52 percent in 2018 (EMVCo, 2019). Other areas of the world have seen an increased use of EMV chip-based cards in that same time frame. In Asia, the percentage of payment card transactions using an EMV chip increased from 19.42 percent in 2014 to 68.15 percent in 2018 (EMVCo, 2014, 2019). One of the reasons the United States lagged behind in implementation of EMV chips has been the existence of other strong antifraud measures that other countries lacked. The existence of these measures alleviated the need for the EMV technology. For countries where such measures were not in place, the need for such technology arose earlier. With the increase in credit card fraud and data breaches in the United States, there has been a need for increased security, and thus EMV chip implementation has become more common (Elkins, 2015).

Although EMV cards are designed to be more secure, cybercriminals are still able to defraud users of such cards. One method cybercriminals can use is a shimmer. A shimmer is a device that is placed inside the payment card slot of a payment terminal (such as an ATM machine or gas pump) that copies the data of cards that are placed in the slot. It is similar to a skimmer—a device that also goes over a payment card slot, but is designed to copy data from magnetic strip-based cards. Although cybercriminals are not able to clone EMV-based cards like they can with magnetic-strip based cards, they can use data from an EMV-based card to create a magnetic strip-based clone of the card (Eddy, 2019). Another method that cybercriminals can use to defraud EMV card users is chip swapping. Cybercriminals may intercept EMV-based cards before they are activated by the owner. The cybercriminals can separate the card, remove the chip and replace it with a fraudulent one, and then glue the card back together. If the victim does not recognize anything wrong with the card, they may activate it. Once it is activated, a cybercriminal can use the chip they removed to access the victim's financial account (Chang, 2018).

There are other uses for chip-based cards. Smart cards have been used in the health-care industry in several countries, including China, France, and Germany. Those cards contain a user's medical records and insurance information (Hansen, 2008). The United States did a test run of health-care smart cards in 2000 and 2001 for those who were receiving government assistance (United States General Accounting Office, 2003). Smart cards have been used in public transit in countries such as Canada and Japan. Those cards contain data on the origin and destination of commuters to calculate the fare owed (Espinoza, et al., 2018;

Nishiuchi and Chikaraishi, 2018). Some countries—such as Germany, Norway, and Switzerland—use smart cards as a form of identification for citizens (Poller et al., 2012). Smart cards have also been used in key cards to access buildings (United States General Accounting Office, 2003). Just as with EMV cards, smart cards used for other functions do have increased security features compared to magnetic strip–based cards. This does not make them invulnerable to attacks from cybercriminals; the information on these cards could be used to the victim's detriment just as having their financial information could. Key cards could be used by cybercriminals to access buildings they are unauthorized to access, and they can then commit theft or other crimes therein. Government identification cards have personally identifying information on them that could be used by a cybercriminal to defraud a victim. Having other personal information about a victim—such as their health care status and travel patterns—would be an invasion of privacy at least, and could be potentially be used for various criminal purposes, such as stalking, extortion, and insurance fraud.

These privacy concerns lead some who develop systems that use chip-based cards to implement additional features to prevent an invasion of privacy. However, in some instances, these increased security measures can create unintended vulnerabilities. For example, one feature of German chip-based citizen identification cards is the lack of a unique authentication key—a feature implemented to prevent the identification of card users by a unique key through the authentication process. Instead, a batch of cards is given identical authentication keys so the key cannot be tied to one user. While this affords an added level of privacy to users, it does make it easier for cybercriminals to use cloned citizen identification cards. If a cybercriminal is able to clone an authentication key, a system authenticating the card with a cloned key would not be able to detect it as a clone, as the system is designed to accept multiple copies of the same authentication key (Poller et al., 2012).

See also: Credit Card Fraud; Personally Identifying Information; Privacy; Skimmer; Vulnerability

Further Reading

Chang, Ellen. 2018. "This new chip-theft scam will blow your mind." Experian, April 24, 2018. https://www.experian.com/blogs/ask-experian/this-new-chip-theft-scam-will-blow-your-mind/

Eddy, Max. 2019. "How to spot and avoid credit card skimmers." *PCMag*, February 6, 2019. https://www.pcmag.com/article/328010/how-to-spot-and-avoid-credit-card-skimmers

Elkins, Kathleen. 2015. "Why it took the US so long to adopt the credit card technology Europe has used for years." *Business Insider*, September 27, 2015. https://www.businessinsider.com/why-it-took-the-us-so-long-to-adopt-emv-2015-9

EMVCo. 2014. "A guide to EMV chip technology." Version 2.0. EMVCo. https://www.emvco.com/wp-content/uploads/2017/05/A_Guide_to_EMV_Chip_Technology_v2.0_20141120122132753.pdf

EMVCo. 2019. "Worldwide EMV deployment statistics." EMVCo. https://www.emvco.com/about/deployment-statistics/

Espinoza, Catalina, Marcela Munizaga, Benjamin Bustos, and Martin Trepanier. 2018. "Assessing the public transport travel behavior consistency from smart card data." *Transportation Research Procedia* 32: 44–53.

Hansen, Margaret M. 2008. "Smart card technology and healthcare information: A dynamic duo." The University of San Francisco. https://repository.usfca.edu/cgi/viewcontent.cgi?article=1009&context=nursing_fac

Nishiuchi, Hiroaki, and Makoto Chikaraishi. 2018. "Identifying passengers who are at risk of reducing public transport use: A survival time analysis using smart card data." *Transportation Research Procedia* 34: 291–298.

Poller, Andreas, Ulrich Waldmann, Sven Vowe, and Sven Turpe. 2012. "Electronic identity cards for user authentication—Promise and practice." *IEEE Security & Privacy* 10, 1: 46–54.

United States General Accounting Office. 2003. *Progress in promoting adoption of smart card technology*. https://www.gao.gov/assets/240/236767.pdf

SNIFFER

A sniffer (sometimes referred to as a packet sniffer or network sniffer) is software that allows one to view the data that travels across a computer network. The software records the data flowing through the network and puts that data in a readable format. It does not interfere with the data through this process (Mitchell, 2019). Sniffers can be used by cybercriminals to capture personally identifying information transmitted across a computer network. This includes the usernames and passwords of a victim, a victim's credit card number, and a victim's social security number—all forms of identity theft. This information can then be used to defraud the victim out of money.

Although sniffers can be used maliciously by cybercriminals, they would not be considered malware. There are legitimate uses for a sniffer. A network administrator can use a sniffer to log and analyze network traffic. Analyzing network traffic helps one determine where bottlenecks in network traffic are occurring so those bottlenecks can be resolved. A sniffer can also be used to diagnose connectivity issues between different computers on the network. Past records kept from a sniffer can be used to help recover the username and password of an authorized network user who has forgotten one or both. Additionally, a sniffer could be used to identify those who are using the network but are unauthorized to do so (Ansari et al., 2003).

There are ways to protect against sniffing by cybercriminals. For network administrators and others who oversee a network, sniffer detection software can be used to determine is a sniffer is operating on the network. For individuals using a network, the use of a VPN—software that encrypts internet traffic before being transmitted over a network—can be used. In such an instance, the data sent can still be captured by sniffer, but the cybercriminal will be unable to read the encrypted data without additional resources to decipher the encryption (Ansari et al., 2003; Mitchell, 2019). Use of Tor—software that can also be used to anonymize one's internet traffic—can potentially be used. Tor works differently than VPNs. Tor utilizes a network of computers, known as nodes. Tor picks a random path of these nodes to go through when a user accesses a server. Tor does use encryption through this process. However, when a Tor user does ultimately connect to its intended network from the exit node—the last node in the chain of random nodes the user was processed through—the operator of that exit node can potentially view the internet traffic of that Tor user. Thus, if an exit node operator (all of whom are volunteers) wants to use a sniffer on the traffic passing through their exit node, they could (Franceschi-Bicchierai, 2015).

Although sniffing generally refers to the monitoring of network traffic, the concept is being expanded to other technological areas. In 2018, Amazon filed a patent that included a "voice sniffer algorithm" that could be used by certain Amazon products with a smart-speaker to sniff and analyze conversations within range of the device. Google has filed similar patents. As with network sniffers, there are legitimate uses for such technology. It appears that Amazon and Google may use the voice sniffer to assist in targeted advertising (Porter, 2019). Just as with network sniffers, however, the technology could ultimately be used for malicious purposes, such as a cybercriminal not only sniffing network traffic for personally identifying information but also potentially sniffing conversions for personally identifying information.

See also: Identity Theft; Malware; Password; Tor (The Onion Router); Virtual Private Network

Further Reading

Ansari, Sabeel, Rajeev S.G., and Chandrashekar H.S. 2003. "Packet sniffing: A brief introduction." *IEEE Potentials* 21, 5: 17–19.

Franceschi-Bicchierai, Lorenzo. 2015. "A researcher used a honeypot to identify malicious Tor exit nodes." *Motherboard*, June 26, 2015. https://motherboard.vice.com/en_us/article/mgbdwv/badonion-honeypot-malicious-tor-exit-nodes

Mitchell, Bradley. 2019. "What is a network sniffer?" *Lifewire*, February 26, 2019. https://www.lifewire.com/definition-of-sniffer-817996

Porter, Tracey. 2019. "Slaves to Google and Amazon—What happens when data reliance gets out of hand?" *Marketing*, February 25, 2019. https://www.marketingmag.com.au/hubs-c/feature-porter-slaves-algorithms-mk1901/

SNOWDEN, EDWARD

Edward Snowden was born in Elizabeth City, North Carolina, on June 21, 1983. In 2006, despite not having a high school diploma, Snowden was hired by the U.S. Central Intelligence Agency (CIA) to work on network security (Burrough and Ellison, 2014). Shortly after hiring him, the CIA put Snowden through its secretive school for those who specialize in technology. After completing the six-month schooling, Snowden was placed on assignment in Geneva, Switzerland (Bamford, 2014). While on assignment, Snowden witnessed the inner workings of the CIA. Given the nature of his job, he had top-secret security clearance and thus had access to inside information (Burrough and Ellison, 2014). What he saw concerned him, though he did not act on that concern at the time (Bamford, 2014). He left employment with the CIA in 2009. Although there is disagreement as to exact reasons why Snowden left, it seems apparent that Snowden was not happy about leaving (see Burrough and Ellison, 2014).

Later in 2009, Snowden found employment with Dell. He initially was assigned to work out of Yokota Air Base—just outside of Tokyo, Japan—with the U.S. National Security Agency (NSA), one of Dell's clients (Bamford, 2014; Burrough and Ellison, 2014). His employment with Dell subsequently took him to Maryland in 2011 and Hawaii in 2012. He continued to work with the NSA in Hawaii, initially as a contractor for Dell but ultimately as a contractor for company Booz Allen (Bamford, 2014). It was while he was employed with Booz Allen that he disclosed top-secret information about the NSA's information-gathering efforts to the public.

The thought of leaking information pertaining to the United States' intelligence collection efforts was something that had been simmering with Snowden for a while. He considered it when employed with the CIA in Geneva. However, he decided against it because he believed that Barack Obama—who had recently been elected president—would run intelligence gathering operations differently once he took office (Bamford, 2014; Burrough and Ellison, 2014). During his subsequent employment as a contractor for the NSA during President Obama's time in office, he observed that nothing had changed since he had worked for the CIA. While working as a contractor for the NSA, Chelsea Manning—an intelligence analyst for the United States army—leaked a substantial number of government documents. These documents were released through WikiLeaks in 2010 and 2011. Although the leaks were made anonymously, Manning's identity was ultimately discovered. Manning was held in custody starting in July 2010 and was eventually sentenced to 35 years in prison in 2013. Seeing how Manning was treated did influence Snowden, who was not eager to be similarly punished (see Burrough and Ellison, 2014). Despite this, Snowden began copying NSA files during this time, starting in the summer of 2012, and began contacting potential journalists to leak the story in December of that same year (Burrough and Ellison, 2014). It appears that what pushed Snowden to finally act was the testimony of James Clapper—director of national intelligence at the time—before a committee of the U.S. Senate. In his testimony in March 2013, Clapper claimed that the NSA did not "wittingly" collect information on United States citizens. Snowden believed Clapper was lying. Based on what Snowden had observed, massive amounts of information were being collected by the NSA. Snowden made plans at this point to leak confidential NSA documents (see Bamford, 2014).

Snowden left Hawaii on May 18, 2013. He took a flight to Hong Kong and took up temporary residence at a hotel in neighboring Kowloon. He reached out to various journalists while in Kowloon. He contacted Glenn Greenwald with the *Guardian*, Barton Gellman with the *Washington Post*, and documentarian Laura Poitras. Greenwald and Poitras ultimately met Snowden at his hotel in Kowloon on June 3 of that year. Just a few days later, both the *Guardian* and the *Washington Post* began publishing stories about the leaks (see Burrough and Ellison, 2014; Greenwald and MacAskill, 2013). After the stories broke, Snowden went into hiding. Julian Assange and Sarah Harrison—both with WikiLeaks—attempted to help Snowden find a safe landing place. Assange had been granted asylum by Ecuador and was in the Ecuadoran embassy in London, avoiding apprehension and extradition himself. Although he was unable to come to Hong Kong to help directly, Harrison was able to. Originally, plans were made for Snowden to seek asylum from Ecuador as well. On June 23, Snowden boarded a flight out of Hong Kong to Moscow along with Harrison. This was to be the first leg of a flight that would ultimately head to Ecuador. However, he never left Russia and has remained there ever since (see Burrough and Ellison, 2014). Russia has granted him a resident permit that is currently good through 2020 (Kramer, 2017).

The full extent of what Snowden leaked is not known. Investigators estimate Snowden had access to roughly 1.7 million documents, with somewhere between 50,000 and 200,000 documents being disclosed to Greenwald and Poitras (Burrough and Ellison, 2014). The exact content of those documents is not known, either. There is some information that we know was contained in Snowden's leaked documents, such as information on Prism—the NSA program that gathered data from technology giants such as Microsoft, Facebook, Apple, and Google (Burrough and Ellison, 2014; Greenwald and MacAskill, 2013). There are other bits of information that have been attributed to Snowden's leaked documents that some believe are from another as-yet-unidentified leaker, such as the fact that the NSA was tapping the phone of German chancellor Angela Merkel (Bamford, 2014).

Opinions of Snowden vary widely. Many view him as a hero. Indeed, he has been the recipient of numerous awards due to his leaking of documents, including the Right Livelihood Award, the Bjørnson Prize, and the Stuttgart Peace Prize (Courage Foundation, 2014a, 2014b, 2015). Others view him as a traitor, as evidenced by his outstanding criminal charges in the United States.

Snowden—if apprehended and extradited to the United States—faces criminal charges for alleged violation of the Espionage Act. If convicted, he could face up to 30 years in prison (Kramer, 2017). There are many who believe Snowden should be pardoned. One petition asking for Snowden's pardon garnered over a million signatures and was supported by the American Civil Liberties Union, Human Rights Watch, and Amnesty International (Morris, 2017). Conversely, many believe Snowden is a criminal and should be turned over to the United States for prosecution. Despite calls for Russia to turn over Snowden by a former acting director of the CIA (see Morell, 2017)—and Russia apparently giving some consideration to the idea (McFadden and Arkin, 2017)—he still remains out of custody in Russia.

In September 2019, Snowden released an autobiography, *Permanent Record*. The United States filed a civil lawsuit against Snowden for publishing the autobiography, which the Department of Justice said is in violation of CIA and NSA nondisclosure agreements.

See also: Assange, Julian; Manning, Chelsea; Privacy; WikiLeaks

Further Reading

Bamford, James. 2014. "Edward Snowden: The untold story of the most wanted man in the world." *Wired*, August 13, 2014. https://www.wired.com/2014/08/edward-snowden/

Burrough, Bryan, and Sarah Ellison. 2014. "The Snowden saga: A shadowland of secrets and light." *Vanity Fair,* April 23, 2014. https://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview

Courage Foundation. 2014a. "Edward Snowden receives 2014 Right Livelihood Honorary Award." September 24. https://edwardsnowden.com/2014/09/24/edward-snowden-receives-2014-right-livelihood-honorary-award/

Courage Foundation. 2014b. "Edward Snowden wins Stuttgart Peace Prize." November 23, 2014.https://edwardsnowden.com/2014/11/24/edward-snowden-wins-stuttgart-peace-prize/

Courage Foundation. 2015. "Edward Snowden wins 2015 Bjørnson Prize." https://edwardsnowden.com/2015/06/02/edward-snowden-wins-2015-bjornson-prize/#more-5504

Greenwald, Glenn, and Ewen MacAskill. 2013. "NSA Prism program taps in to user data of Apple, Google and others." *The Guardian*, June 7, 2013. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Kramer, Andrew E. 2017. "Russia extends Edward Snowden's asylum." *New York Times*, January 18, 2017. https://www.nytimes.com/2017/01/18/world/europe/edward-snowden-asylum-russia.html

McFadden, Cynthia, and William Arkin. 2017. "Russia considers returning Snowden to U.S. to 'curry favor' with Trump: Official." *NBC News*, February 11, 2017. https://www.nbcnews.com/news/us-news/russia-eyes-sending-snowden-u-s-gift-trump-official-n718921

Morell, Michael J. 2017. "Putin's perfect gift." *The cypher brief*, January 15, 2017. https://www.thecipherbrief.com/column/agenda-setter/putins-perfect-gift-1095

Morris, David Z. 2017. "Campaign to pardon Edward Snowden delivers 1 million signatures to President Obama." *Fortune*, January 14, 2017. http://fortune.com/2017/01/14/pardon-snowden-campaign/

Snowden, Edward. 2019. *Permanent record.* New York: Metropolitan Books.

SOCIAL ENGINEERING

Social engineering is the process of deceiving people into divulging information that is personal or confidential, often for the purpose of defrauding those people. It can also include deception that leads someone to carry out an act that would grant the social engineer access to a place or thing they would not have been able to access before.

While social engineering often involves infiltration of online accounts and networks to defraud victims, social engineering efforts can take place offline as well as online. A social engineer can obtain information from documents in a victim's unlocked car, a victim's garbage, and various other places (Heary, 2009). A social engineer can use this information in conjunction with information obtained online (such as information from a victim's social media accounts) to attempt to gain access to the victim's accounts.

Just as the efforts used to get a victim's information can be done offline as well as online, the access to a restricted account or area can be offline as well as online. Online, a social engineer can use a victim's username and password to gain entry to a bank account. Offline, a social engineer could befriend a victim, use that confidence to gain access to their home, and then steal cash from the victim's home.

There are several tactics that social engineers can use to defraud a victim. Common tactics include phishing (soliciting personal information from someone via e-mail), pretexting (using a concocted story to elicit personal information from someone), and baiting (luring someone to provide personal information in exchange for some benefit to them). Whichever method is used, there is a general pattern to how social engineering takes place. The social engineer will first formulate an attack, gather information, prepare to carry out the attack, establish a relationship with the intended victim, exploit the relationship with the victim, and then debrief (Mouten et al., 2016). The debriefing can serve to allay concerns the victim might feel about disclosing sensitive information (Mouten et al., 2016).

Some of most notorious hacks have been accomplished through social engineering. The hack suffered by Sony was accomplished through a common phishing scheme (Elkind, 2015). The hack of e-mails from members of the Democratic National Committee before the 2016 U.S. election was accomplished—at least in part—through phishing as well (Swaine and Roth, 2018). A hack of the U.S. Department of Justice was accomplished through a mix of phishing and pretexting (Cox, 2016).

See also: Awareness; Financial Crimes; Fraud; Identity Theft; Phishing; Social Media; Sony Pictures Entertainment Hack

Further Reading

Cox, Joseph. 2016. "Hacker plans to dump alleged details of 20,000 FBI, 9,000 DHS employees." *Motherboard*, February 7, 2016. https://motherboard.vice.com/en_us/article/9a3y4e/hacker-plans-to-dump-alleged-details-of-20000-fbi-9000-dhs-employees

Elkind, Peter. 2015. "Sony Pictures: Inside the hack of the century, part 2." *Fortune*, June 26, 2015. http://fortune.com/sony-hack-part-two/

Heary, Jamey. 2009. "Top 5 social engineering exploit techniques." *PC World*, November 14, 2009. https://www.pcworld.com/article/182180/top_5_social_engineering_exploit_techniques.html

Mouton, Francois, Louise Leenan, and H. S. Venter. 2016. "Social engineering attack examples, templates and scenarios." *Computers and Security* 59: 186–209.

Swaine, Jon, and Andrew Roth. 2018. "US indicts 12 Russians for hacking DNC emails during the 2016 election." *The Guardian*, July 13, 2018. https://www.theguardian.com/us-news/2018/jul/13/russia-indictments-latest-news-hacking-dnc-charges-trump-department-justice-rod-rosenstein

SOCIAL MEDIA

Social media refers to the various internet-based platforms that allow users to interact with each other. These interactions include generally include messaging and the sharing of pictures and videos. Other features include the ability for users to create a profile providing information about themselves, the ability to forward on the comments of others, and the ability to flag ("like") favorable content. Certain social media platforms have a specific niche. For example, LinkedIn is specifically designed for occupational networking, and Twitch is specifically designed for livestreaming video games and other content. Common social media platforms in the United States include Facebook, YouTube, Twitter, and Instagram.

Andrew Weinreich and Adam Seifer—a lawyer and a copywriter, respectively—created the first recognized social media site, Six Degrees, in 1997. At its peak, Six Degrees had millions of users (Boyd and Ellison, 2007). Worldwide, there are now hundreds of different social media sites. It is estimated that the number of social media users worldwide is over 2.5 billion. It is worth noting that not all social media sites operate worldwide. For example, several popular social media sites (e.g., Facebook, Twitter, Instagram) have been banned in China (Yuan, 2018). In 2018, it appeared that Facebook was going to be allowed in the country, but the preliminary approval that Facebook appeared to have was quickly revoked (Mozer, 2018).

Social media presents unique challenges when it comes to cybercrime. Just as with e-mail and other electronic communications, social media can be used to defraud users. In its direct form, scammers can solicit users to either send money or provide personal information, which can then be used to defraud them. Scams via social media have an added layer of concern in that users often provide personal information to social media sites as part of their user profiles. While it is generally possible for a user to restrict who may view their profile, not all users implement these restrictions. Even for users who do implement restrictions, determined scammers may be able to hack into user profiles and view the information anyway. Armed with the personal information of a user, a scammer can paint a more convincing tale to induce a user to send them money or divulge further personal information.

Social media can be used to indirectly defraud users. Those looking to influence public opinion can create numerous fake social media accounts, and then use those accounts to make it look like a large number of people support a certain product or position. Those accounts could all "like" or "follow" a certain company or product on a social media platform, making that company or product look more popular than it actually is. Not only does this misrepresent how many people actually like a company or product, but it can also cause the profile for that company or product to come up more frequently in searches on the social media platform. Also, public opinion can be swayed when certain stories are shared en masse by these fraudulent accounts.

This is what is believed to have happened with Russian hackers and the 2016 U.S. election. Russian hackers created fake accounts on popular social media platforms and posted stories and opinions that seemed designed to influence the election (Office of the Director of National Intelligence, 2017). It appears that Russian hackers may have used these same methods to sway public opinion of the movie *Star Wars: The Last Jedi* (Bay, 2018). This was apparently done to further sow discord in American society by criticizing the movie's depiction of gender, race, and social class issues as left-leaning.

It is not just financial crimes that can take place via social media sites. Crimes such as threatening, harassment, intimidation, and stalking can also take place. Where these crimes are communication-based, they can be committed online just as easily as in person. The anonymity afforded by the internet can make it difficult to find a perpetrator who wishes to stay anonymous and has taken the steps to remain so, but the acts are criminal nonetheless.

Social media can also be used to keep the public appraised of public unrest. There have been various political protests that have been coordinated using social media, and those protests have resulted in conduct that was deemed illegal by the countries in which those protests took place. Social media was widely used during the events of the Arab Spring and is believed to have had an impact on how those events unfolded (Howard et al., 2011). As mentioned above, several popular social media sites are banned in China. The ban appears to be in response to the Urumqi riots in China and the use of social media to disseminate information about the riots (Blanchard, 2009).

It is important to note that law enforcement can use information from social media profiles as evidence in a criminal case. Communications made via a social media platform can be obtained. Entire profiles can be obtained if they contain relevant evidence. For example, if a suspect posts pictures or videos depicting a crime they committed, law enforcement could obtain this information. If a suspect has not restricted who can view their profile, and the information is public, law enforcement will be able to obtain this information simply by conducting an internet search. As for information that has been restricted by users, law enforcement can still obtain it. However, they will likely have to subpoena it from the social media company.

See also: China; Hate Crime; Health Care, Effects on; Identity Theft; Russia

Further Reading

Bay, Morten. 2018. "Weaponizing the haters: *The Last Jedi* and the strategic politicization of pop culture through social media manipulation." *ResearchGate*. https://www.researchgate.net/publication/328006677_Weaponizing_the_haters_The_Last_Jedi_and_the_strategic_politicization_of_pop_culture_through_social_media_manipulation

Blanchard, Ben. 2009. "China tightens Web screws after Xinjiang riot." *Reuters*, July 6, 2009. https://www.reuters.com/article/us-china-xinjiang-internet/china-tightens-web-screws-after-xinjiang-riot-idUSTRE5651K420090706

Boyd, Danah M., and Nicole B. Ellison. 2007. "Social network sites: Definition, History, and Scholarship." *Journal of Computer-Mediated Communication* 13, 1: 210–230.

Howard, Philip N., Aiden Duffy, Deen Freelon, Muzammil Hussain, Will Mari, and Marwa Mazaid. 2011. "Opening closed regimes: What was the role of social media during the Arab Spring?" Seattle: University of Washington.

Mozer, Paul. 2018. "China said to quickly withdraw approval for new Facebook venture." *New York Times*, July 25, 2018. https://www.nytimes.com/2018/07/25/business/facebook-china.html

Office of the Director of National Intelligence. 2017. *Assessing Russian activities and intentions in recent U.S. elections*. Washington, D.C.: Office of the Director of National Intelligence.

Yuan, Li. 2018. "A generation grows up in China without Google, Facebook or Twitter." *New York Times*, August 6, 2018. https://www.nytimes.com/2018/08/06/technology/china-generation-blocked-internet.html

SONY PICTURES ENTERTAINMENT HACK

Just before Thanksgiving in 2014, hackers were able to break into the computer systems of Sony Pictures Entertainment. Company employees found the computers were locked and the screens displayed a red skull with the message that said "Hacked by #GOP." The hacking group referred to themselves as the "Guardians of Peace." Three days before the event, the hackers had sent company executives an e-mail from "God's Apostles" in which they threatened to "bombard" the company if they were not given money. The message said, "The compensation for it, monetary compensation we want. Pay the damage, or Sony Pictures will be bombarded as a whole. You know us very well. We never wait long. You'd better behave wisely" (Robb, 2015). During the event, the company's Twitter accounts were also seized.

The hackers used malware to get into the Sony system. Once they gained access, the group accessed many confidential documents. The hackers made many of those company secrets public, including embarrassing company e-mails sent from top executives. Some of those e-mails referred to actress Angelina Jolie as a "minimally talented spoiled brat" (Beaumont-Thomas, 2014). There were also e-mails that included racist comments about President Barack Obama. The attackers also released a script for an unreleased James Bond movie. Possibly more damaging was the release of personal information found in SONY databases. The hackers made personal contracts available to the public. The hackers released private employee information, including home addresses, social security information, health records, and financial information. Hackers also released information about salaries and bonuses, performance reviews, criminal background checks, medical conditions, passport information, and retirement or termination records.

That year, Sony finished a satirical movie about North Korean leader Kim Jong-un, titled *The Interview*. The hackers demanded that Sony not release the film because it depicted Kim's assassination. They threatened to carry out violent acts if theaters showed the movie. As a result, many theaters across the country refused to show the movie. Initially, Sony canceled any plans to release the film but instead made it available through an online format. People wanted to see the movie, and they also wanted to show the hackers that their threats of violence were not going to stop people from seeing the film. In four days, the movie was rented or purchased two million times. Many independent theaters opted to show the movie despite the threats. Many of the viewings were sold out (Seal, 2015).

In addition to the threats against the company for *The Interview* and the release of company information, the hackers destroyed the company's computer servers. The company was forced to pay an estimated $35 million to repair the infrastructure so employees could once again access their computers.

Some officials in the U.S. government immediately blamed North Korean government hackers, with some officials voicing opinions that the attack was a terrorist act. Officials from North Korea denied any involvement. Nonetheless, President Obama reported that the North Koreans were responsible for the attack. On January 2, 2015, Obama issued an Executive Order mandating new sanctions against the government of North Korea.

In the days after the attack, officials from Sony reached out to the FBI and other law enforcement agencies. As a way to mitigate any public embarrassment, Sony contacted other media outlets and requested that they refrain from downloading any additional leaked data and that they destroy any stolen data that they already possessed. In addition, Sony tried to block any further distribution of the stolen data.

Computer security firms, including Symantec, Kaspersky Lab, Carbon Black, RiskIQ, and Novetta, conducted another investigation into the origin of the attack. Their final report indicated that the hackers were a group referred to as the Lazarus Group, an organization that is still actively hacking. According to the security companies, the members of this group were also allegedly responsible for a series of cyberattacks in 2009 on websites in both the United States and South Korea (Zetter, 2016). The group members have attacked computer systems in various industries, governments, media, and critical infrastructure sites in places such as Taiwan, China, Japan, and India. They seem to be more interested in stealing information and monitoring the activities of these agencies as opposed to causing harm.

There were some lasting repercussions from the hacking event. In the days after the hacking, the co-chairman of Sony Pictures, Amy Pascal stepped down from her job in the company. It was estimated that the attack could cost the company tens of millions of dollars (Miller and Hamedy, 2014). Executives at SONY were forced to rebuild their damaged computer networks and pay for any legal bills that result from damages to reputations of the actors involved. In addition, there were disruptions to ongoing projects that were underway at the company. Officials had to devote a great deal of time and attention to rebuilding the company's reputation with the public so as not to lose their customer base.

In April 2017, Adam Mudd was sent to jail for charges related to the hacking. Mudd, a teenager and known computer hacker, developed a hacking program, called the Titanium Stresser program, that was used to carry out the attacks. He pleaded guilty in England to charges including the commission of unauthorized acts with intent to impair the operation of computers; making, supplying, or offering to supply an article for use in an offense in violation of the Computer Misuse Act; and concealing criminal property (Press Association, 2017).

The Sony attack served as a wake-up call to many regarding the seriousness of cyber-attacks. It raised awareness by other companies, government agencies, and individuals about the vulnerabilities of their networks and the need to increase security. Many companies, agencies and individuals increased their network security systems in the days and weeks after the attack.

In the final analysis, the cyberattack on Sony caused millions of dollars in property damage to the company and great embarrassment to its management. Some people lost their jobs. The attack could have been a blow to freedom of expression in the United States, but that did not happen (Schwartz, 2014). These events caused many other companies to increase their security to prevent a similar attack on their networks. It is recognized that a similar attack could happen again at any time.

See also: Cyberterrorism; Economy, Effects on; Entertainment, Effects on; Malware

Further Reading

Beaumont-Thomas, Ben. 2014. "Angelina Jolie called 'minimally talented spoiled brat' in hacked Sony emails." *The Guardian*, December 10, 2014. https://www.theguardian.com/film/2014/dec/10/sony-hack-eamils-angelina-jolie-scott-rudin-amy-pascal-david-fincher

Miller, D., and Hamedy, S. 2014. "Cyberattacks could cost Sony Pictures tens of millions of dollars." *Los Angeles Times*, December 5, 2014. http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-hacking-cost-20141205-story.html

Press Association. 2017. "Teenage hacker jailed for masterminding attacks on Sony and Microsoft." *The Guardian*, April 25, 2017. https://www.theguardian.com/technology/2017/apr/25/teenage-hacker-adam-mudd-jailed-masterminding-attacks-sony-microsoft

Robb, D. 2015. "The Sony hack one year later: Just who are the Guardians of Peace?" *Deadline*, November 24, 2015. http://deadline.com/2015/11/sony-hack-guardians-of-peace-one-year-anniversary-1201636491/.

Schwartz, Yishai. 2014. "Why aren't we retaliating right now for the Sony Cyberattack?" *New Republic*, December 19, 2014. https://newrepublic.com/article/120604/sony-interview-hack-demands-us-cyberattack-response

Seal, M. 2015. "An exclusive look at Sony's hacking saga." *Vanity Fair*, March. https://www.vanityfiar.com/hollywood/2015/02/sony-hacking-seth-rogan-evan-goldberg

Zetter, K. 2016. "The Sony hackers were causing mayhem years before they hit the company." *Wired*, February 24, 2016. https://www.wired.com/2016/02/sony-hackers-causing-mayhem-years-hit-company/

SPAM

Spam are unsolicited or unwanted messages sent to someone via the internet or other form of electronic communication. The term comes from the name of a brand of canned meat that was first introduced in 1937. The product has been parodied by several, though a parody done by Monty Python in the 1970s appears to have been the impetus for associating this term with unwanted communications (MacNaughton et al., 1970). The first time this association appears to have been made was in 1993 in response to hundreds of copies of the same message being accidentally posted to a website (McWilliams, 2004, p. 309).

While the first association of the term "spam" with unwanted electronic messages occurred in 1993, the dissemination of unwanted electronic messages predates this. The earliest example of modern spam occurred in 1978. Gary Thuerk sent several hundred unsolicited advertisements to recipients via ARPANET, a computer network used by the United States military that predated the internet (Fletcher, 2009). It appears that as early as 1864, telegraph lines were used to send unsolicited advertisements (Anonymous, 2007; Fletcher, 2009). The first noted instance was that of a dentist, Messrs Gabriel, sending an unsolicited advertisement for his dentistry to British politicians (Anonymous, 2007).

Spam is often associated with unwanted e-mail, but spam can be any unwanted electronic message. There are terms that refer to specific types of spam. Spit refers to unwanted messages received via internet telephone (acronym: spam over internet telephone), and spim refers to spam received via instant message (acronym: spam over instant message).

Spam is a widespread problem. It has been estimated that 88 percent of e-mails globally are spam (Rao and Reiley, 2012). The problem extends beyond the annoyance caused by spam. It has been estimated that spam costs Americans $20 billion annually (Rao and Reiley, 2012).

In the United States, the CAN-SPAM Act was passed in 2003 to combat the problems brought about by spam. The Act requires companies that send out advertisements via e-mail to disclose that the e-mail is an ad. It also requires companies to allow people to opt out of receiving e-mails in the future. Violations of this law can result in financial penalties for companies (Federal Trade Commission, 2009).

There can be criminal repercussions for spammers who use spam as a means of committing some existing fraud, such as fraud and theft. An example of this is the 2017 arrest of Peter Yuryevich Levashov—a Russian spammer who had been operating for years. Levashov would offer to send out millions of spam messages for his customers in exchange for money. The amount would vary depending on the content of the spam. Spam for counterfeit goods would go for $200 a million, where spam pushing phishing attacks—e-mails trying to fraudulently elicit personal information from recipients—went for $500 a million (Graff, 2017). He pleaded guilty on September 12, 2018, to offenses in the United States tied to his spamming, as well as other cybercrimes tied to his distribution of malware and stealing login information of victims (United States Department of Justice, 2018).

See also: Advanced Research Projects Agency Network; CAN-SPAM Act of 2003; E-mail-related Crimes; Fraud; Phishing

Further Reading

Anonymous. 2007. "The etiquette of telecommunications: Getting the message, at last." *The Economist*, December 13, 2007. https://www.economist.com/node/10286400/print?story_id=10286400

Federal Trade Commission. 2009. "CAN-SPAM Act: A compliance guide for business." https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

Fletcher, Dan. 2009. "Spam." *Time*, November 2, 2009. http://content.time.com/ time/business/article/0,8599,1933796,00.html

Graff, Garrett M. 2017. "How the FBI took down Russia's spam king—And his massive botnet." *Wired*, April 11, 2017. https://www.wired.com/2017/04/fbi-took-russias-spam-king-massive-botnet/

MacNaughton, Ian (director), Graham Chapman (writer), John Cleese (writer), Terry Gilliam (writer), Eric Idle (writer), Terry Jones (writer), and Michael Palin (writer). 1970. Season 2, Episode 12 in *Monty Python's Flying Circus*. London: BBC.

McWilliams, Brian. 2004. *Spam kings: The real story behind the high-rolling hucksters pushing porn, pills and @*#?% enlargements*. Cambridge, UK: O'Reilly.

Rao, Justin M., and David H. Reiley. 2012. "The economics of spam." *Journal of Economic Perspectives* 26, 3: 87–110.

United States Department of Justice. 2018. "Russian national who operated Kelihos botnet pleads guilty to fraud, conspiracy, computer crime and identity theft offenses." September 12, 2018. https://www.justice.gov/opa/pr/russian-national-who-operated-kelihos-botnet-pleads-guilty-fraud-conspiracy-computer-crime

SPOOFING

In the context of cybercrime, spoofing is where something is disguised to appear to be something it is not. Spoofing is used by cybercriminals to enable them to commit cybercrime. There are several different types of cyber spoofing, including e-mail spoofing, DNS spoofing, caller ID spoofing, IP spoofing, and GPS spoofing (Malwarebytes, 2019).

E-mail spoofing is where an e-mail is sent that appears to come from one source, but in fact has been sent by another source. This form of spoofing can be used by cybercriminals to steal personally identifying information from victims. This is done through a phishing attack. The cybercriminal sends an e-mail that appears to be from a legitimate source: an established business, a government agency, and so forth. The e-mail, under the guise of being a legitimate entity making a legitimate request, will ask the victim to provide personally identifying information, such as their login credentials, social security number, or birthdate. If a victim falls for the ruse, the cybercriminal can obtain the personally identifying information and use it to steal money from the victim. E-mail spoofing can also be used to spread malware. The tactic is generally the same. A cybercriminal will send an e-mail to the victim, posing as a legitimate source. In these instances, however, the cybercriminal asks the victim to open an attachment or click on a link in the e-mail. If the victim does so, the attachment or link will actually download malware on the victim's computer. While a spoofed e-mail claiming to be from a friend of the victim may raise red flags if the cybercriminal asks for personally identifying information, a spoofed e-mail from a friend asking the victim to click on a link to an interest news article, for example, might not (Malwarebytes, 2019).

Caller ID spoofing is where someone makes it appear that they are calling from a phone number other than the one they are actually calling from. Similar to the e-mail spoofing, caller ID spoofing can be used to trick a victim into thinking a call is coming from a legitimate entity, such as a business or government agency. If the victim believes the call is actually from a legitimate entity, they may divulge personally identifying information to the cybercriminal spoofing the call. Another tactic cybercriminals use when caller ID spoofing is neighborhood spoofing. This is where the cybercriminal spoofs the number to appear to be coming from the neighborhood of the victim by making the area code and first three numbers of the number the same as the victim's phone number. This is done to increase the likelihood of a victim answering the phone (Federal Communications Commission, 2019). These calls can be used to gather personally identifying information as well. They could also be used to capture the voice of a victim. If the victim verbally responds to questions asked by the cybercriminal over the phone—especially those that ask for a "yes" or "no" response—a cybercriminal could record those responses and use them as a voice signature to authorize a money transfer from the victim's bank over the phone (Federal Communications Commission, 2019; Tatham, 2019).

IP spoofing occurs when someone alters the IP address of their computer to appear to be a different IP address. By doing this, a cybercriminal can obfuscate where a cyberattack is actually coming from, making it difficult for law enforcement and others to track down where the attack actually came from. IP spoofing can also be used to circumvent security measures employed by computer networks that only allow trusted computers—computers with an IP address that the network recognizes as having permission—to access the network. If a cybercriminal is able to spoof the IP address of their computer to make it appear to be a trusted computer, they can access networks they would otherwise be unable to (Kaspersky, 2019).

IP spoofing also permits a person to spoof the physical location of the computer. With location spoofing, a person has their computer or other electronic device indicate that it is accessing the internet from a physical location different from the one it is actually accessing the internet from. This is often done through the use of a VPN. Where a VPN serves as an intermediary between a user and the website they are ultimately accessing, the website being accessed ascertains the user's location via that user's representation of their location through the VPN. Location spoofing is used to access internet content that is unavailable in their geographic location. Indeed, circumventing censorship is an advertised feature of some VPNs (ExpressVPN, 2019). An example of this can be seen in China. China censors the internet within its borders via the Great Firewall of China. A user in China that wishes to circumvent the Great Firewall can use a VPN. By listing their location as something other than China (i.e., spoofing their location), the user can access the internet without those restrictions. It is a crime to circumvent internet restrictions in this way in China. Since 2017, several people providing and using VPN services in China have been sentenced to prison for their actions (Banjo and Chen, 2019). Location spoofing is also commonly used to circumvent geo-blocking. Geo-blocking is where an entertainment company restricts the geographic areas from which certain content may be viewed. As each country has its own copyright laws, entertainment companies will employ geoblocking to avoid running afoul of those laws, only permitting the content to be viewed in countries where those companies have secured the rights to show it. One study found that avoiding geoblocking was the primary motivation for people to use VPNs, with nearly half of VPN users indicating that was their motivation (Valentine, 2018). Those who use location spoofing to avoid geoblocking are likely acting illegally. Entertainment companies, such as Netflix and HBO, prohibit the circumvention of geoblocking in their terms of service (HBO, 2019; Netflix, 2019). Violating the terms of service can give rise to a civil cause of action against the violator. However, it is possible that the violator could also face criminal charges. As noted in HBO's terms of service: "If you choose to access [material] from other locations you do so on your own initiative and at your own risk. You are responsible for complying with local laws, if and to the extent local laws are applicable" (HBO, 2019). In other words, if a user illegally accesses copyrighted material, and the laws of the country in which the user resides treats that illegal access as a crime, that user may face criminal charges in addition to a civil cause of action from the entertainment company.

GPS spoofing is similar to location spoofing. Instead of changing one's location through a VPN, however, GPS spoofing changes the actual GPS coordinates of an electronic device capable of being traced via GPS. GPS spoofing can be used to circumvent services that are GPS-dependent. For example, some games playable on cell phones are dependent on GPS, such as *Pokémon Go*. The location of items in the game is tied to the GPS location of the phone. By using GPS spoofing, a player can trick the game into thinking the phone is at a specific GPS location, and the player can collect the item tied to that location (Malwarebytes, 2019). Use of GPS spoofing in *Pokémon Go* is considered a violation of the terms of service (Niantic, 2019). Where the game offers the in-game purchase of items, if GPS spoofing were used to obtain items in a manner that would alleviate the player's need to purchase those items, it could be considered theft. GPS spoofing can potentially be used for other purposes as well. In 2011, the Iranian military was able to spoof the GPS coordinates of a U.S. drone. By doing so, the drone landed at a location it thought was its home base in Afghanistan but was actually in Iran. This permitted the Iranian military to study the technology of the drone once it was intercepted (Peterson and Faramarzi, 2011).

See also: China; Copyright Infringement; Domain Name System Cache Poisoning; Malware; Personally Identifying Information; Phishing; Spoofing; Virtual Private Network

Further Reading

Banjo, Shelly, and Lulu Yilun Chen. 2019. "Digital dissidents are fighting China's censorship machine." *Bloomberg Businessweek*, June 3, 2019. https://www.bloomberg.com/news/articles/2019-06-03/digital-dissidents-are-fighting-china-s-censorship-machine

ExpressVPN. 2019. "How to change your location in Google Chrome." ExpressVPN. https://www.expressvpn.com/support/troubleshooting/spoof-location-google-chrome/

Federal Communications Commission. 2019. "Caller ID spoofing." https://www.fcc.gov/consumers/guides/spoofing-and-caller-id

HBO. 2019. "HBO terms of use." https://www.hbo.com/terms-of-use

Kaspersky. 2019. "What is IP spoofing?" https://usa.kaspersky.com/resource-center/threats/ip-spoofing

Malwarebytes. 2019. "Spoofing." https://www.malwarebytes.com/spoofing/

Netflix. 2019. "Netflix terms of use." https://help.netflix.com/en/legal/termsofuse

Niantic. 2019. "Niantic Terms of Service." https://nianticlabs.com/terms/en/

Peterson, Scott, and Payam Faramarzi. 2011. "Exclusive: Iran hijacked US drone, says Iranian engineer." *Christian Science Monitor*, December 15, 2011. https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer

Tatham, Matt. 2019. "The ultimate list of the year's worst scams." Experian, March 11, 2019. https://www.experian.com/blogs/ask-experian/the-ultimate-list-of-the-years-worst-scams/

Valentine, Olivia. 2018. "VPNs are primarily used to access entertainment." Global Web Index, July 6, 2018. https://blog.globalwebindex.com/chart-of-the-day/vpns-are-primarily-used-to-access-entertainment/

SPYWARE

Generally speaking, spyware is software that gathers information about the user of a computer without the consent of the user, and it transmits that information to someone else. The precise definition of spyware is not universally agreed upon. One area of disagreement centers on what constitutes consent. Some software may gather information about its users—either directly or through software bundled with it—and this is disclosed in an end user license agreement that comes with the software. The question in these instances becomes whether informing users about information gathering through an end user license agreement is sufficient. The concern is that such a method may be too indirect, and thus such users cannot truly be said to have consented to the software gathering data and sending it to the makers of the software (Federal Trade Commission, 2005). Another area of disagreement centers on the degree of harm this type of software must cause before it is considered to be spyware. Some believe the software must actually cause some sort of harm—be malware—to be considered spyware. Others maintain that all software that gathers data without the consent of the user is, per se, spyware because the nonconsensual gathering of data is harmful in and of itself (Federal Trade Commission, 2005).

Spyware can be used for a multitude of reasons. One piece of spyware (known as Turla or Uroburos) targeted computers belonging to governments that are members of NATO—including the United States—in an apparent attempt at cyber espionage. The spyware gained attention in 2014 but had been under observation by some security companies for years prior to this. Although it has not been definitively determined, many believe this spyware was created and disseminated by Russia (Reuters, 2014). A similar attack was carried out by China to infiltrate not only the computers of foreign governments but also the computers of foreign companies. China did this not through software but rather through hardware. Evidence of this attack began to emerge in 2015. That year, Amazon was considering the acquisition of Elemental Technologies, a creator of video-compression software. As part of a preacquisition investigation of Elemental Technologies by Amazon, it was discovered that the servers used by Elemental Technologies contained small microchips on the motherboards that were not part of the original schematic for the motherboards. These servers were manufactured for Elemental

Technologies by Super Micro Computer, a company based in the United States that subcontracted at least some of the manufacture of their servers to companies in China. It is believed that the additional, undisclosed microchips were added to the motherboards by the PLA (the Chinese military) during manufacture in China. The servers were used by several U.S. agencies, including the CIA, the Department of Defense, and the navy. The servers were also used by several large corporations, including Amazon and Apple. It is believed the added microchip permitted China to monitor the usage of the computer within which it was installed (Robertson and Riley, 2018).

In addition to being used by governments to engage in governmental and business espionage, spyware can be used by individuals for more personal reasons. There are companies that sell spyware to individuals. For some of these companies, the spyware is pitched as a means to catch a cheating spouse. Indeed, spyware appears to be used frequently in domestic cases. In 2014, one survey found that 75 percent of the domestic violence shelters they contacted housed victims whose phone conversations had been eavesdropped by their abusers (Shahani, 2014). The use of spyware to monitor people in this manner is generally illegal. However, the marketers of this software will include language—whether on their website, in an end user license agreement, or other method—indicating the software is intended for legal uses only (Cox, 2017; Shahani, 2014).

There are certain types of software that are arguably spyware. Adware, depending on how it operates, could fall into this category. Adware is software that displays advertisements to users. This can be incorporated as a side function of some other software, such as a web browser. In some instances, adware will gather data from a user (such as web browsing history) to tailor the advertisements displayed to the user's interests. If the user has not consented to that information being gathered, the adware could be classified as spyware (see Federal Trade Commission, 2005). Certain types of DRM software may fall into the category of spyware. In 2006, Microsoft designed a tool—Windows Genuine Advantage Notifications—that would verify that the Windows operating system installed on a computer was obtained legitimately. The software did send information back to Microsoft, though the company maintained that the information sent was not meaningful information. The company did note it had not been as forthcoming as it could have been about the software and what it did (Evers, 2006). Sony BMG employed similar—yet seemingly more invasive—DRM methods in 2005. The company would download software onto the computers of those who purchased certain CDs from them. Neither the fact that the software had DRM functionality nor that it would be downloaded on a user's computer was included in the end user license agreement provided by Sony BMG (Russinovich, 2005). The software also captured information concerning a user's listening habits even though the end user license agreement claimed such information would not be captured (Electronic Frontier Foundation, 2019). Sony BGM faced numerous lawsuits over the implementation of this software (Associated Press, 2005; McMillan, 2006).

In some instances, law enforcement may use spyware in their investigations. Federal law enforcement has used keystroke monitors to track the computer habits of suspected criminals, and law enforcement may also use devices to surreptitiously intercept the cell phone communications (see McCullagh, 2007; Siegel, 2017). The collection of such information in the United States by law enforcement would have to comply with the search and seizure requirements of the Fourth Amendment of the U.S. Constitution as well as other applicable laws. A concern law enforcement may have when authorized to use spyware by a court is whether the suspect's antimalware software will catch the spyware and delete it. Some private antimalware companies have indicated that, if they were ordered by a court, they would not tell a customer of the presence of government-installed spyware. However, antimalware companies that were asked if they have ever received such an order either denied they had, indicated they did not know if they had, or did not answer the question. Nonetheless, there is some indication that one such company (McAfee) contacted the FBI in 2001 to make sure its antimalware software would not interfere with the FBI's spyware (McCullagh, 2007).

See also: Digital Rights Management; End User License Agreement; Malware; Rootkit

Further Reading

Associated Press. 2005. "Sony BMG tentatively settles suits on spyware." *New York Times*, December 30, 2005. https://www.nytimes.com/2005/12/30/technology/sony-bmg-tentatively-settles-suits-on-spyware.html

Cox, Joseph. 2017. "I tracked myself with $170 smartphone spyware that anyone can buy." *Motherboard*, February 22, 2017. https://motherboard.vice.com/en_us/article/aeyea8/i-tracked-myself-with-dollar170-smartphone-spyware-that-anyone-can-buy

Electronic Frontier Foundation. 2019. "Sony BMG litigation info." https://www.eff.org/cases/sony-bmg-litigation-info

Evers, Joris. 2006. "Microsoft's antipiracy tool phones home daily." *CNet*, June 8, 2006. https://www.cnet.com/news/microsofts-antipiracy-tool-phones-home-daily/

Federal Trade Commission. 2005. *Monitoring software on your PC: Spyware, adware, and other software*. https://www.ftc.gov/sites/default/files/documents/reports/spyware-workshop-monitoring-software-your-personal-computer-spyware-adware-and-other-software-report/050307spywarerpt.pdf

McCullagh, Declan. 2007. "Will security firms detect police spyware?" *CNet*, July 17, 2007. https://www.cnet.com/news/will-security-firms-detect-police-spyware/

McMillan, Robert. 2006. "Sony rootkit settlement reaches $5.75M." PCWorld, December 22, 2006. https://www.pcworld.com/article/128310/article.html

Reuters. 2014. "Suspected Russian spyware in Europe, US attacks." *CNBC*, March 7, 2014. https://www.cnbc.com/2014/03/07/suspected-russian-spyware-in-europe-us-attacks.html

Robertson, Jordan, and Michael Riley. 2018. "The big hack: How China used a tiny chip to infiltrate U.S. companies." *Bloomberg Businessweek*, October 4, 2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Russinovich, Mark. 2005. "Sony, rootkits and digital rights management gone too far." *Microsoft TechNet* (blog), October 31, 2005. https://blogs.technet.microsoft.com/markrussinovich/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far/

Shahani, Aarti. 2014. "Smartphones are used to stalk, control domestic abuse victims." National Public Radio, September 15, 2014. https://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims

Siegel, Robert. 2017. "Local police departments invest in cell phone spy tools." National Public Radio, February 17, 2017. https://www.npr.org/2017/02/17/515841069/local-police-departments-invest-in-cell-phone-spy-tools

STATE ACTOR

A state actor is someone who works for or on behalf of the government. When looking at cyberattacks, knowing whether the attack was perpetrated by a state actor could have an impact on whether the attack is treated as a cybercrime or as a warfare matter (Flatow, 2011; Stoll, 2018). Additionally, the distinction between a state actor and a non-state actor matters in the context of criminal investigations and the maintenance of the rights of suspects.

State actors carry out and are the victims of cyberattacks with some regularity, with hundreds of such attacks occurring between 2006 and 2019 (Center for Strategic and International Studies, 2019). The use of the internet for military objectives is an open field, with state actors still figuring out the contours of what types of attacks could be carried out via cyber means (Kallberg and Thuraisingham, 2013). In instances where different state actors use cyberattacks against each other, it might be expected those attacks would be treated as a warfare matter. However, this does not generally appear to be the case. The Center for Strategic and International Studies (2019) put it this way:

> If Chinese or Russian spies had backed a truck up to the State Department, smashed the glass doors, tied up the guards and spent the night carting off file cabinets, it would constitute an act of war. But when it happens in cyberspace, we barely notice.

Although these cyberattacks are not generally treated as acts of war, there are instances where they have been treated as criminal matters in the United States. For example, the United States indicted 12 Russian officers for interfering with the 2016 presidential election (Prokop, 2019). Moves like these seem to be largely political, as it is not expected that the country that sponsored the cyberattack will cooperate with the extradition of those who were indicted for their role in the attack.

The other instance where the distinction between a state actor and a nonstate actor has significance in relation to cybercrime is in the enforcement of laws prohibiting cybercrime. In the United States, the distinction between a state actor and a nonstate actor is important when it comes to the rights granted to citizens under the Constitution. Specifically, where the government is responsible for maintaining the rights of the citizens, only state actors can be held liable for infringing those rights. In the context of criminal law, these Constitutional rights include the right against unreasonable search and seizure (Fourth Amendment), the right against self-incrimination (Fifth Amendment), and the right to an attorney (Sixth Amendment).

The most common state actor a person would encounter when dealing with a criminal case would be a law enforcement officer, such as a police officer or a Federal Bureau of Investigation (FBI) agent. Thus, law enforcement officers are responsible for assuring that someone accused of a crime has their Constitutional rights honored. If a law enforcement officer violates a citizen's rights, there are repercussions. Perhaps the most common consequence of law enforcement violating a citizen's rights in a criminal case is suppression of the evidence (e.g., the state is prohibited from using the illegally obtained evidence in a trial against the suspect whose rights were violated). In some instances, a suspect who had their rights violated might file a civil lawsuit against the department of the officer that violated their rights. The officer who violated a suspect's rights might face criminal prosecution themselves, depending on the flagrancy of the violation. These rights must be honored for those suspected of cybercrimes just as much as they must be honored for someone suspected of any other crime.

By contrast, a nonstate actor is not obligated to uphold a citizen's Constitutional rights. A non-state actor is anyone who does not work for the state. This is true even if the person in question has responsibilities similar to a law enforcement officer. For instance, a loss prevention officer for a department store or a security officer for a concert venue would not be considered state actors. Both positions have duties similar to a law enforcement officer, such as crime apprehension and order maintenance. However, people in both positions are employed by private businesses, not the state.

Although nonstate actors are not obligated to uphold the Constitutional rights of citizens, this does not mean there are no consequences for the actions of nonstate actors. For example, if a loss prevention officer breaks into the car of a suspected shoplifter looking for evidence, that officer could potentially be sued civilly or prosecuted for a crime just as a state actor could, albeit under different statutes in most instances. The pertinent difference is that any evidence found in the car by the loss prevention officer could still be used against the shoplifter. If a police officer (a state actor) were to do the same thing, the evidence could not be used against the shoplifter.

It is possible that a nonstate actor could be deemed to be an agent of (i.e., working for) a state actor, and this would make that agent responsible for upholding a citizen's constitutional rights just the same as the state actor they work for. An example of this would be the use of an undercover informant. That informant would be no more able to conduct an illegal search of someone's dwelling than the officer they work for.

As mentioned above, Constitutional rights in the criminal justice system apply just as much in the cyber world as they do anywhere else. Thus, if a law enforcement officer wanted to conduct a search of someone's hard drive for evidence of a crime, they would first need to obtain a warrant just as they would if they wanted to search someone's house for evidence of a crime. Likewise, nonstate actors would not be obligated to uphold citizens' constitutional rights in the cyber world. For example, if a private e-mail provider or social media company wanted to take the information of one of its customers and provide it to the government as evidence in a criminal case, that evidence could be used against that customer as long as the e-mail provider or social media company was not working at the direction of the government. As mentioned above, there could be other repercussions for the e-mail provider or social media company even though they are nonstate actors. However, suppression of the customer's information in a criminal case would not be one of those remedies.

See also: Federal Bureau of Investigation; International Issues; Privacy

Further Reading

Center for Strategic and International Studies. 2019. "Significant cyber incidents." https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

Flatow, Ira. 2011. "Cyberattacks may be 'acts of war.'" National Public Radio, June 3, 2011. https://www.npr.org/2011/06/03/136925541/cyber-attacks-may-be-acts-of-war

Kallberg, Jan, and Bhavani Thuraisingham. 2013. "State actors' offensive cyberoperations: The disruptive power of systematic cyberattacks." *IT Professional* 15, 3: 32–35.

Prokop, Andrew. 2019. "All of Robert Mueller's indictments and plea deals in the Russia investigation." Vox, March 22, 2019. https://www.vox.com/policy-and-politics/2018/2/20/17031772/mueller-indictments-grand-jury

Stoll, Richard J. 2018. "Is a cyberattack an act of war?" *Houston Chronicle*, July 26, 2018. https://www.houstonchronicle.com/local/gray-matters/article/russia-cyberattacks-act-of-war-military-force-13107824.php

STORM BOTNET

The Storm botnet was a botnet that was put into operation in 2007. It derived its name from the news headline included in the spam messages used to disseminate it: storms sweeping across Europe. The botnet was designed to infect computers running Microsoft Windows. At its peak, the Storm botnet had infected between 500,000 and 1,000,000 computers and was distributing roughly 20 percent of all spam worldwide (Keizer, 2008b; Leyden, 2008).

The Storm botnet was relatively short-lived. There appeared to be some pushback from the operators of the botnet against those trying to get rid of it. Some researchers studying the botnet were hit with DDoS attacks, knocking them offline for days. Whether this was a programmed function of the botnet or the actions of those operating it is unknown (Greene, 2007). Nonetheless, Microsoft focused its efforts on eradicating the botnet during the latter part of 2007 and was able to put a sizeable dent in the number of computers that were infected with it. In the course of a few months, Microsoft had removed the botnet from roughly 526,000 computers that had been infected with it. By early 2008, it was estimated that only 85,000 were infected with the botnet, and it was distributing only 2 percent of all spam worldwide (Keizer, 2008b; Leyden, 2008). The botnet appeared to be essentially extinct by the end of 2008 (Leyden, 2008).

It has been suspected that the RBN was behind the Storm botnet (Keizer, 2008b). The St. Petersburg–based company did fade from public view at about the same time the Storm botnet began to fade (Keizer, 2008a; Warren, 2007). Peter Yuryevich Levashov, a resident of St. Petersburg, was indicted in the United States for his use of several botnets—the Storm botnet included—to commit cybercrimes such as theft of login credentials, bulk spam distribution, and use of ransomware. Levashov did plead guilty to some charges in the United States in 2018, but those charges related to his use of the Kelihos botnet, not the Storm botnet (United States Department of Justice, 2018).

Though it appears the Storm botnet is dead, some believe the botnet was not so much killed as abandoned. As noted above, it is suspected the RBN was behind the Storm botnet. Some believe that just as the RBN attempted to diversify the locations it operated from in late 2007, so too did the type of botnets diversify at that point. Thus, the decline in computers infected by the Storm botnet—while in part due to the efforts of Microsoft—was the result of cybercriminals trying to avoid detection by expanding the types of botnet they were using (Keizer, 2008a). Although there appears to be some disagreement regarding whether Microsoft's efforts eradicated the Storm botnet or it was abandoned, there appears to be agreement that whoever was behind that Storm botnet is still likely committing cybercrime via different botnets (Keizer, 2008a, 2008b; Leyden, 2008). Indeed, it appears that botnets similar to the Storm botnet were in operation after the Storm botnet was assumed dead. In 2010, researchers found three botnets that appeared to be variants of the Storm botnet (Goodin, 2010).

See also: Bots and Botnets; Distributed Denial-of-Service Attack (DDoS); Ransomware; Russian Business Network; Spam

Further Reading

Goodin, Dan. 2010. "Infamous Storm botnet rises from the grave." *Register*, April 27, 2010. https://www.theregister.co.uk/2010/04/27/storm_botnet_returns/

Greene, Tim. 2007. "Storm worm strikes back at security pros." *Networkworld*, October 24, 2007. https://www.networkworld.com/article/2287530/storm-worm-strikes-back-at-security-pros.html

Keizer, Gregg. 2008a. "Microsoft didn't crush Storm, counter researchers." *Computerworld*, April 24, 2008. https://www.computerworld.com/article/2536817/microsoft-didn-t-crush-storm--counter-researchers.html

Keizer, Gregg. 2008b. "Microsoft: We took out Storm botnet." *Computerworld*, April 22, 2008. https://www.computerworld.com/article/2536783/microsoft--we-took-out-storm-botnet.html

Leyden, John. 2008. "Storm botnet blows itself out." *The Register*, October 14, 2008. https://www.theregister.co.uk/2008/10/14/storm_worm_botnet_rip/

United States Department of Justice. 2018. "Russian national who operated Kelihos botnet pleads guilty to fraud, conspiracy, computer crime and identity theft offenses." September 12, 2018. https://www.justice.gov/opa/pr/russian-national-who-operated-kelihos-botnet-pleads-guilty-fraud-conspiracy-computer-crime

Warren, Peter. 2007. "Hunt for Russia's web criminals." *The Guardian*, November 15, 2007. https://www.theguardian.com/technology/2007/nov/15/news.crime

STUXNET, *see* OPERATION OLYMPIC GAMES

SUPERVISORY CONTROL AND DATA ACQUISITION

Supervisory Control and Data Acquisition (SCADA) is a system used to monitor and control industrial equipment (e.g., sensors, motors, valves). It does so through the use of hardware elements—hardware either integrated into the industrial equipment (e.g., a valve) or the equipment itself (e.g., a sensor)—that are digitally connected to the SCADA software at a computer terminal (Inductive Automation, 2018). As industrial equipment can be controlled by this SCADA setup, industrial equipment is vulnerable to cyberattacks.

Although the acronym "SCADA" did not come into existence until the 1970s, the use of computers to monitor and control industrial equipment started in the 1950s. Around the turn of the century, SCADA systems transitioned to be open in their software design, permitting system components from one SCADA manufacturer to work with components from another. With advances in technology, SCADA systems in 2019 permit real-time data from hardware components to be accessible to authorized personnel worldwide (Inductive Automation, 2018).

There have been cyberattacks carried out against SCADA systems. The first malware designed to attack SCADA systems was the Stuxnet worm (Kushner, 2013). In a SCADA system, the industrial equipment is often run through a programmable logic controller (PLC), which in turn connects to the computer system with the SCADA software (Inductive Automation, 2018). A PLC runs automated processes for the hardware (Schneier, 2010). Stuxnet was designed to affect a specific PLC made by the German company Siemens. This had led to the belief that Stuxnet was designed with a specific target in mind (Schneier, 2010). Several people, including the Iranian government and several computer security experts, believe the United States and Israel worked together to use Stuxnet to bring down the Natanz nuclear facility in Iran in 2010. This belief is based on several factors, including an internal investigation conducted by Iran and the absence of denials from the United States and Israel in regard to the attacks (Dehghan, 2011). Stuxnet was used to cause the SCADA system to direct the centrifuges at the nuclear facility to spin faster than they were supposed to. This damaged the centrifuges (Warrick, 2011). Iran accused Siemens of facilitating the attack against it by providing the United States and Israel with information about its PLCs that were being used in the Iranian nuclear facility (Dehghan, 2011).

There have been other cyberattacks on SCADA systems. In 2016, hackers gained access to the computer system of a water treatment plant in the United Kingdom. The hackers were able to chance the levels of certain chemicals that were added to the water at the plant (Leyden, 2016). An assessment of the attack led investigators to conclude that the hackers apparently did not have a working knowledge of SCADA systems, as their attacks seemed to lack understanding of how the water flow system worked. Also, of the four times the hackers attempted to manipulate the system, only twice were they able to actually to change the amount of chemicals released into the water (Leyden, 2016).

See also: Hacker and Hacking; International Issues; Malware; Worm

Further Reading

Dehghan, Saeed Kamali. 2011. "Iran accuses Siemens of helping launch Stuxnet cyber-attack." *The Guardian*, April 17, 2011. https://www.theguardian.com/world/2011/apr/17/iran-siemens-stuxnet-cyber-attack

Inductive Automation. 2018. "What is SCADA?" https://inductiveautomation.com/resources/article/what-is-scada

Kushner, David. 2013. "The real story of Stuxnet." *IEEE Spectrum*, February 26, 2013. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Leyden, John. 2016. "Water treatment plant hacked, chemical mix changed for tap supplies." *The Register*, March 24, 2016. https://www.theregister.co.uk/2016/03/24/water_utility_hacked/

Schneier, Bruce. 2010. "The story behind the Stuxnet virus." *Forbes*, October 7, 2010. https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html#10aa31d951e8

Warrick, Joby. 2011. "Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack." *Washington Post*, February 16, 2011. http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html

SUPERZAPPING

Superzapping is a technique that can be used by cybercriminals to bypass all the security features on a computer network. The term "superzapping" is derived from a program developed by International Business Machines (IBM) known as Superzap. The Superzap program has features that can be beneficial to network administrators. It is often used by administrators to patch executable programs. This can save an administrator the hassle of having to reinstall an entire executable program to fix a relatively small bug in the programming (IBM Knowledge Center, 2010). If there is a malfunction on a computer network—even a malfunction that cannot be corrected through standard recovery methods or restart methods—Superzap can be used to work around those issues. In that regards, it becomes a convenient last resort method for network administrators to resolve difficult network problems (Knotts and Richards, 1989; Parker, 1989). Superzap is not the only program that can do this. There are several other programs that have the same functionality as Superzap (see Parker, 1989). The Superzap program has become the term used to describe such programs in general.

While the use of Superzap and similar programs is legal in many instances, the unauthorized use of those programs can be criminal. The term "superzapping" refers to those instances where Superzap or a similar program is used in an unauthorized fashion (Romney, 1995). Where superzapping permits a user to bypass all the standard security measures in place on a computer network, it is an effective tool for a cybercriminal to use to hack into a computer network. In addition to permitting a cybercriminal to bypass all the standard security measures in place, superzapping may not leave behind evidence that files have been manipulated by the cybercriminal, making detection of the activities of the cybercriminal difficult (Parker, 1989).

Where superzapping can be a powerful tool in a cybercriminal's arsenal, regulating the availability and use of Superzap and similar programs becomes important for network administrators to prevent unauthorized use of them. Indeed, superzapping may unintentionally be made available to a cybercriminal when network administrators fail to see superzapping as a threat and thus fail to secure Superzap or similar programs (Kabay, 2002; Parker, 1989). There are various security measures that have been suggested to secure these programs. In order to keep the programs off the network itself, thus assuring it is not generally available to anyone who accesses the network, it has been suggested that the programs be kept in a physical safe. Also, where employees of a company with access to these programs could potentially use them for criminal purposes, it has been suggested that the implementation of a policy that requires two employees to authorize the use of Superzap or a similar program could reduce the likelihood of those programs being used against the company (Kabay, 2002).

See also: Bypass; Hacker and Hacking; Tools

Further Reading

IBM Knowledge Center. 2010. "SPZAP (a.k.a. Superzap): Dynamically update programs or data." IBM. https://www.ibm.com/support/knowledgecenter/zosbasics/com.ibm.zos.zdatamgmt/zsysprogc_utilities_SPZAP.htm

Kabay, M.E. 2002. "Controlling superzapping." *Computer World*, February 8, 2002. https://www.computerworld.com.au/article/20959/controlling_superzapping/

Knotts, Rose, and Tom Richards. 1989. "Computer security: Who's minding the store?" *The Academy of Management Executive* 3, 1: 63–66.

Parker, Donn B. 1989. *Computer crime: Criminal justice resource manual*. United States Department of Justice. https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf

Romney, Marshall. 1995. "Computer fraud—What can be done about it?" *The CPA Journal* 65, 5, pp. 30–34.

SWARTZ, AARON (1986–2013)

Aaron Swartz was a computer programmer and hacker who was best known for downloading over four million articles from JSTOR, an online organization that stores and provides access to academic journals. He was charged with multiple felonies, including wire fraud, unlawfully obtaining information from a protected computer, and recklessly damaging a protected computer. He was also an activist who fought against social injustice. Swartz died on January 11, 2013, by suicide.

Aaron Hillel Swartz was born in 1986 in Illinois. His father worked in the software industry as the founder of the firm Mark Williams Company, giving Aaron an insight into the industry at an early age. As a teenager, Swartz won an award for creating a noncommercial website. Upon graduating from high school, he chose to attend Stanford University, where he worked on Infogami, a way to create websites. After his freshman year, he did not return to Stanford but instead continued to work for Infogami. The company merged with Reddit in November 2005 and formed a new firm called Not a Bug, which the owner of *Wired* magazine then acquired. Swartz initially began to work on *Wired* but left the company after a short time. He chose to become a computer programmer and political activist.

In September 2007, Swartz was part of a group that created a new firm, Jottit. The following year, he downloaded almost 2.7 million federal court documents, with the goal of making them available to the general public. The FBI investigated Swartz for this activity, but no charges were filed.

After this experience, Swartz chose to assist in the creation of the Progressive Change Campaign Committee, which sought to provide support for progressive government policies such as health care reform. He also agreed to be a cofounder of Demand Progress, an organization that provided encouragement to individuals who wanted to get involved in supporting civil liberties and other related policies. In these positions, Swartz actively campaigned to show his opposition to a proposed law called the Stop Online Piracy Act, which was introduced into Congress in 2011 and sought to deter people from violating copyright laws. Swartz and other critics claimed that the law would make it easier for law enforcement to shut down websites run by people who were accused of breaking the law. The proposed bill did not pass.

Because of his expertise in computers and technology, Swartz became a research fellow at Harvard University's Safra Research Lab on Institutional Corruption. In 2010 and 2011, using his research fellow account from his position at Harvard University, Swartz used the network from Massachusetts Institute of Technology (MIT) to download hundreds of academic journal articles from JSTOR, an online repository for academic articles and manuscripts. The amount Swartz downloaded far exceeded the maximum amount allowed. Once they were downloaded, he posted the articles on the internet, a violation of copyright laws.

A U.S. Secret Service agent and MIT police arrested Swartz in January 2011 near the campus of Harvard University on charges of breaking and entering, wire fraud, computer fraud, unlawfully obtaining information from a protected computer, and recklessly damaging a protected computer. He was also charged with acts related to the Computer Fraud and Abuse Act of 1986 (CFAA).

If convicted of the charges, Swartz was facing a possible fine of up to $1 million, with a possible 35 years in prison. In addition to these penalties, Swartz would be forced to forfeit any assets, pay restitution, and spend time on supervised release. The prosecutors offered Swartz a plea bargain that would have required him to serve six months in a federal minimum security prison if he pleaded guilty to 13 federal crimes. Swartz rejected the offer and proposed a counteroffer, but the prosecution rejected it so Swartz sought to have a trial.

Many of Swartz's supporters claimed that the federal government charged Swartz far more severely simply as a means to ensure his punishment. To show support for Swartz, the hacking group Anonymous launched a DoS attack against the Department of Justice.

Before the trial started, Swartz took his own life on January 11, 2013, by hanging himself in his apartment in Brooklyn, New York. Upon his death, the federal prosecutors dropped all charges against him.

Not long after Swartz's death, U.S. Representative Zoe Lefgren (D-CA) proposed a bill (HR 2454/S1196) she called Aaron's Law. She explained that the government relied on some vague wording in the laws to argue that violating the service's user agreement or terms of service of the online service (in this case, JSTOR) was a violation of the CFAA. Further, Lefgren argued that this interpretation of the law may result in many ordinary activities being considered criminal, resulting in high penalties. Lefgren's proposal would exclude violations of terms of service from the CFAA. Even though the bill had significant support from other members of Congress, it stalled in committee and was not passed. The proposal was reintroduced in May 2015 as HR 2454/S1030, but it failed to pass again.

After Swartz's suicide, his family and friends accused U.S. Attorney General Eric Holder and the Department of Justice for cracking down on Swartz too hard by overcharging him and threatening him with extreme prison time if he did not plead guilty. While Holder expressed sympathy to Swartz's family, he described the case as a "good use of prosecutorial discretion" (Holpuch, 2013). Others claim the case was delayed for too long simply as a way to punish Swartz even more and also because of his political activism. In 2013, Swartz was posthumously inducted into the Internet Hall of Fame.

See also: Computer Fraud and Abuse Act of 1986; Hacker and Hacking

Further Reading

Day, Elizabeth. 2013. "Aaron Swartz: Hacker, genius . . . martyr?" *The Guardian*, June 1, 2013. https://www.theguardian.com/technology/2013/jun/02/aaron-swartz-hacker-genius-martyr-girlfriend-interview

Holpuch, Amanda. 2013. "Attorney General Holder defends Aaron Swartz hacking prosecution." *The Guardian*, March 7, 2013. https://www.theguardian.com/technology/2013/mar/07/eric-holder-defends-aaron-swartz-hacking-prosecution

MacFarquhar, Larissa. 2013. "Requiem for a dream." *The New Yorker*, March 11, 2013. https://www.newyorker.com/magazine/2013/03/11/requiem-for-a-dream

Peter, Justin. 2016. *The idealist: Aaron Swartz and the rise of free culture on the internet*. New York: Scribner.

Scheiber, Noam. 2013. "The inside story of why Aaron Swartz broke into MIT and JSTOR." *The New Republic*, February 13, 2013. https://newrepublic.com/article/112418/aaron-swartz-suicide-why-he-broke-jstor-and-mit

Swartz, Aaron. 2015. *The boy who could change the world: The writings of Aaron Swartz*. New York: The New Press.

SWATTING

Swatting is the practice of calling for the police to respond to the home of someone else under false pretenses. The term "swatting" is derived from the fact that a SWAT

(Special Weapons and Tactics) team will often show up to respond to the false report. In many instances, the victims of swatting are people who do live streams of video games. By making a false report to law enforcement, people watching the live stream online will be able to watch the person's house get stormed by the police. Swatting is generally intended as a prank. However, swatting is illegal. Someone who swats another person could be guilty of false reporting to law enforcement, misuse of 911, or a similar charge.

Swatting can be dangerous. In one incident in Wichita, Kansas, swatting resulted in someone's death. In that case, two teenagers were playing *Call of Duty*. One of the teenagers, Casey Viner, became upset with the other, Shane Gaskill, and enlisted a third person, Tyler Barriss, to swat Gaskill. Gaskill caught wind of what was going on and provided Viner and Barriss with an old address where he no longer lived. Barriss called the police and claimed he had committed a murder and was holding another person hostage. He gave the police the old address Viner had given them. The police responded to the old address. The residents there were not aware of what was going on. Andrew Finch, age 28 at the time, was shot and killed by officers when he answered the door. Gaskill, Viner, and Barriss were all charged with federal crimes arising from the incident. Barriss, the man who made the actual call to the police, was charged with involuntary manslaughter in state court (Burgess, 2017; Chokshi, 2018).

This incident in Wichita was not Barriss's first time swatting. Barriss was charged with multiple federal crimes for other swatting incidents he had been involved in prior to the Wichita case. In some of those instances, it is alleged that others would pay Barriss to swat someone. Three other people were charged with federal crimes for soliciting Barriss to carry out swats for them, all in 2017 (Helsel and Blankstein, 2019). While in custody on charges for the Wichita incident, Barriss was able to access the internet through an inmate kiosk at the Sedgwick County Jail in Kansas. He logged into one of his Twitter accounts and threatened to swat more people (Crecente, 2018).

Barriss pleaded guilty to 51 federal charges related to his swatting activity. This included three counts stemming from the Wichita incident—false information and hoaxes, cyberstalking, and conspiracy. He also pleaded guilty to two counts of making bomb threats against the Federal Communication Commission and the FBI on December 14, 2017, and December 22, 2017, respectively. The remaining 46 counts were for earlier swatting incidences and unauthorized use of credit cards. Among the 46 charges he pleaded to were charges of making interstate threats and conspiracy to commit bank fraud (Leiker, 2018). As of early 2019, Barriss's state charge of involuntary manslaughter is unresolved, as are the federal charges against his two codefendants, Gaskill and Viner.

There are other cases of swatting that have resulted in force being used by law enforcement against unsuspecting victims. On February 18, 2005, two men—Zachary Lee of Maryland and Robert Walker-McDaid of Coventry, England—made plans to swat Tyran Dobbs. Walker-McDaid made the call from England to a U.S. terrorism hotline, posing as Dobbs. He claimed to be armed and have hostages. When the SWAT team arrived, Dobbs was shot in the face and chest with rubber bullets. Dobbs's facial bones were broken, and his lungs were bruised (Kentish, 2017). Lee pleaded guilty to conspiracy to provide false information and false information and hoax on November 7, 2017 (United States Attorney's Office, District of Maryland, 2017). Walker-McDaid's case appears to be outstanding as of early 2019.

Several celebrities has been swatted. Ashton Kutcher and Justin Bieber were both swatted by a 12-year-old boy in October 2013 (Duke, 2013). Other swatted celebrities include Russell Brand, Mylie Cyrus, and Justin Timberlake. David Hogg—one of the survivors of the shooting at Stoneman Douglas High School in Parkland, Florida—was also swatted in 2018, though he was out of town at the time it happened (Fagan 2018).

It is estimated that there are 400 instances of swatting that occur every year, with an average cost to law enforcement of $10,000 per incident (Burgess, 2017).

See also: Cyberbullying; Doxing

Further Reading

Burgess, Katherine. 2017. "Swatting is 'a potentially deadly crime' that's become 'extraordinarily common.'" *The Wichita Eagle*, December 29, 2017. https://www.kansas.com/news/local/article192152254.html

Chokshi, Niraj. 2018. "3 men face federal charges in fatal 'swatting' prank." *New York Times*,May24,2018.https://www.nytimes.com/2018/05/24/us/gamers-swatting-charges.html

Crecente, Brian. 2018. "Inmate awaiting trial in fatal swatting case gets online, threatens to swat again." *Variety*, April 10, 2018. https://variety.com/2018/gaming/news/inmate-swatting-case-tweets-1202749320/

Duke, Alan. 2013. "Boy admits 'swatting' Ashton Kutcher, Justin Bieber." CNN, March 12, 2013. https://www.cnn.com/2013/03/11/showbiz/kutcher-swatting-conviction/index.html

Fagan, Kaylee. 2018. "Everything you need to know about 'swatting,' the dangerous so-called 'prank' of calling a SWAT team on someone." *Business Insider*, June 5, 2018. https://www.businessinsider.com/what-does-swatting-mean-2015-3

Helsel, Phil, and Andrew Blankstein. 2019. "3 charged in 'swatting' cases connected to man charged in death of Kansas man." *NBC News*, January 23, 2019. https://www.nbcnews.com/news/us-news/3-charged-swatting-cases-connected-man-charged-death-kansas-man-n962026

Kentish, Benjamin. 2017. "British man charged after U.S. gamer is shot by Swat police following hoax terrorism call." *The Independent*, April 10, 2017. https://www.independent.co.uk/news/uk/home-news/robert-mcdaid-charged-tyran-dobbs-swatting-hoax-call-swat-terrorism-maryland-shot-gun-explosives-a7677071.html

Leiker, Amy Renee. 2018. "Tyler Barriss, who made fatal swatting call in Wichita, guilty of 51 federal charges." *The Wichita Eagle*, November 13, 2018. https://www.kansas.com/news/local/crime/article221616115.html

United States Attorney's Office, District of Maryland. 2017. "Catonsville man pleads guilty to conspiracy in 'swatting' incident." United States Attorney's Office, District of Maryland, November 7, 2017. https://www.justice.gov/usao-md/pr/catonsville-man-pleads-guilty-conspiracy-swatting-incident

SYMANTEC

Symantec is a Mountain View, California-based cybersecurity company known for producing antivirus and data management programs. The name is a combination of the words "syntax," "semantics," and "technology." Originally founded in 1982 by Gary Hendrix as a way to learn more about artificial intelligence, it was one of the first tech companies to focus on fighting computer viruses. Two years after the company's startup, C&E Software acquired Symantec, but retained the company's original name. One of Symantec's first products, Q&A, was very successful. The company also released an antivirus program for Apple computers that sold over $100,000 in its first month. Then it began to purchase existing products and companies. By 1988, Symantec sold 20 different products. In 1990, Symantec merged with Peter Norton Computing and decided to focus on the development of antivirus programs that could be used not only by large companies but also by home computer users with little knowledge of computers. The company's antivirus and data management programs are sold under the Norton name (Norton, n.d.).

Not long after that, Symantec purchased Certus Corporation, which produced the Novi Antivirus software, and then the Peter Norton Computing Company. This allowed Symantec to sell an antivirus software program to the general public. When the Melissa virus was released, many organizations relied on Symantec antivirus software to keep their computers safe.

Symantec products include both Norton Internet Security and Symantec Endpoint Protection. Both programs are types of security software, but they are geared toward different groups. The Norton division includes Norton Antivirus, Norton Internet Security, and Norton 360. These programs detect malware and viruses on networks. They also include e-mail spam filtering and methods to identify phishing attempts. Endpoint Protection has products for both small businesses and those that have over 100 employees. The software is sold as a box copy or can be downloaded.

In 1999, some of the employees of technology investment firm Battery Ventures, along with Ted Julian, an expert in the security and technology field, created @stake that developed security software as well as offered consulting services and training. In 2000, the company acquired L0pht Heavy Industries and Cerberus Information Security Limited, an internet security firm. In 2004, Symantec bought @stake, a California-based company that provides network security services. Many experts in computer security were employed by the new company, including former Cult of the Dead Cow member Peiter Zatko, AKA Mudge, and Chris Wysopal, also known as Weld Pond.

The company continues to grow and expand as they acquire companies that have expertise in protecting computer systems and data. In 2004, the company released L0phtCrack, a password auditing system that identifies weak passwords that people often use, such as birthdays or a spouse's or child's name, and changes passwords if needed to delete suspicious accounts. In August 2005, Symantec acquired another software security company, Sygate. Starting in November 2005, all Sygate personal firewall products were no longer available to customers. In 2007, Symantec acquired Altiris, which produces software management programs, and Vontu, a company that specializes in data loss prevention. The following year, Symantec executives agreed to acquire three new companies, PC Tools, AppStream Inc., and MessageLabs. In 2010, Symantec officials made public their plans to acquire PGP Corporation and GuardianEdge, and then they acquired Rulespace later that year. In 2011, they obtained Clearwell Systems, and in 2012 they acquired LiveOffice, a company that managed cloud storage and backup systems. They also bought Odyssey Softwary and Nukona Inc. in 2012.

In 2014, officials at Symantec announced that it had plans to divide into two publicly traded companies. One company would provide expertise on security and the other on information management. The latter company (Veritas Technologies) was then sold to the Carlyle Group. NitroDesk Inc. joined Symantec in 2014.

Symantec continues to develop technology to help keep computers and networks safe. In 2016, it announced a program to help protect cars that are connected to the internet against zero-day attacks. Officials in the company made an announcement in November 2016 that it was acquiring the identity theft–protection company LifeLock for a cost of $2.3 billion. It also acquired Blue Coat Systems in 2016. Then in August 2017, officials announced that Symantec was selling the side of the company that verifies the identity of websites, and on January 4, 2018, they announced a new agreement with BT Enterprises to create endpoint security protection.

Even with all of the changes, the company continues to provide customers with technology to keep their computers and their data safe. They provide consulting and education services to those who need it, but they also offer a variety of programs to protect people and companies from becoming victims of an attack.

See also: Banking Attacks; Melissa Worm; Virus

Further Reading

Bank, David, Dennis Berman, and Don Clark. 2004. “Symantec could strike a deal to buy Veritas by end of week.” *Wall Street Journal*, December 15, 2004. https://www.wsj.com/articles/SB110303773243299658

Norton. n.d. “Pioneers in security.” https://us.norton.com/how-we-protect-you/heritage-since-1982/

Reuters. 2016. “Symantec to buy Blue Coat for $4.7 billion to boost enterprise unit.” CNBC, June 13, 2016. https://www.cnbc.com/2016/06/13/symantec-to-buy-blue-coat-for-47-billion-to-boost-enterprise-unit.html

Richmond, Riva. 2001. “Symantec banks on integrated security systems.” *Wall Street Journal*, September 25, 2001.

Roman, Jeffrey. 2014. “Symantec revamps security offerings: Experts ponder whether anti-virus market is ‘dead.’” *Bank Info Security*, May 6, 2014. https://www.bankinfosecurity.com/symantec-revamps-security-offerings-a-6818

Schubert, Christina. n.d. “The evolution of Norton 360: A brief timeline of cyber safety.” https://us.norton.com/internetsecurity-how-to-the-evolution-of-norton-360-a-brief-timeline-of-digital-safety.html

Symantec. 2004. “Symantec to acquire @stake.” https://www.symantec.com/about/newsroom/press-releases/2004/symantec_0916_03

SYRIAN ELECTRONIC ARMY

The Syrian Electronic Army is a hacker group that is supportive of Syrian president Bashar al-Assad. Assad became the president of Syria in July, 2000. At that time, he was elected to a seven-year term. Since then, Assad has been reelected to two additional seven-year terms, in 2007 and in 2014. In March 2011, a civil war broke out in Syria. The catalyst for this civil war appears to be the detainment of boys who had put graffiti critical of Assad and the Syrian government on the walls of their school. Protests followed the incarceration of these youths, and the Syrian government began to use military force to dispel these protests (Stracqualursi and Kelsey, 2017). It was around this same time that the Syrian Electronic Army first emerged. In April, 2011, it started a Facebook page. That page was quickly taken down by Facebook. Over the next several weeks, the Syrian Electronic Army attempted to start a total of 18 different Facebook pages, all of which were taken down by Facebook. In May 2011, it launched its own website (Norman, 2019). That website described the Syrian Electronic Army as "a group of enthusiastic Syrian youths who could not stay passive towards the massive distortion of facts about the recent uprising in Syria" (Smith-Spark, 2013).

The Syrian Electronic Army appears to deny that it is working at the behest of the Assad-led government (Fowler, 2013; Noman, 2019). Indeed, as of early 2019, there appears to be no direct evidence to show that the Syrian Electronic Army is being directed in that way. However, there is evidence that would indicate the Assad-led government tacitly supports it. The Syrian government authorized the registration of the Syrian Electronic Army's website, and hosted it until June, 2013 (Fowler, 2013; Noman, 2019). Assad has voiced support and appreciation for the Syrian Electronic Army, as have Syrian-government-run media outlets (Fowler, 2013; Noman, 2019).

In its first few years of operation, the Syrian Electronic Army primarily engaged in website vandalism and DDoS attacks. These attacks were directed toward the websites and social media accounts of those opposed to the Assad-led government and the websites and social media accounts of organizations in Western countries in general (Noman, 2019). Those attacked include CBS, MPR, BBC, al-Jazeera, and FIFA (Fowler, 2013). In addition to these attacks, spam campaigns were directed by the Syrian Electronic Army against the Facebook pages of similar organizations and individuals. The organizations and individuals whose Facebook pages were attacked include Barack Obama, Nicolas Sarkozy, Oprah Winfrey, al-Arabia TV, the European Union, Human Rights Watch, and Sheikh Yusuf Al Qaradawi (Noman, 2019). The attacks of the Syrian Electronic Army have escalated past website vandalism. In 2013, the *New York Times* website was attacked. The Syrian Electronic Army was able to not only vandalize the website of the *New York Times* but was also able to gain control of the website's domain name, shutting the site down for 20 hours (Smith-Spark, 2013). In late 2018, information emerged that the Syrian Electronic Army was working on using spyware called SilverHawk on Android devices to track the activities of those they wished to target (Brewster, 2018).

The exact membership of the Syrian Electronic Army is unknown. Although the group claims to be composed primarily of Syrians, its use of online recruitment methods means that members could be from anywhere there is an internet connection (Smith-Spark, 2013). There are a handful of members whose identities have been discovered. They are Ahmad Umar Agha (known as The Pro online), Firas Dardar (known as The Shadow online), and Peter Romar. Agha and Dardar were added to the Federal Bureau of Investigation's Cyber Most Wanted list in 2016 (Federal Bureau of Investigation, 2016). Romar was extradited to the United States from Germany in 2016 and pleaded guilty to conspiring to receive extortion proceeds and conspiring to unlawfully access computers (United States Department of Justice, 2016). Romar was given credit for time served as his sentence (Weiner, 2018). Agha and Dardar have been charged with multiple felonies in the United States, including wire fraud, identity theft, and conspiracies related to computer hacking. However, as of early 2019, both still remain at large and are believed to be in Syria (Federal Bureau of Investigation, 2016; Weiner, 2018). There are other members of the Syrian Electronic Army that have been discovered, though they are known only by their online names, such as Medo Coder and Raddex (Brewster, 2018).

See also: Distributed Denial-of-Service Attack (DDoS); Federal Bureau of Investigation; Hacker and Hacking; Political Uses; Social Media; Spam; Vandalism

Further Reading

Brewster, Thomas. 2018. "Syrian Electronic Army hackers are targeting android phones with fake WhatsApp attacks." *Forbes*, December 5, 2018. https://www.forbes.com/sites/thomasbrewster/2018/12/05/syrian-electronic-army-hackers-are-targeting-android-phones-with-fake-whatsapp-attacks/#1d7f0df66ce4

Federal Bureau of Investigation. 2016. "Syrian cyber hackers charged." March 22, 2016. https://www.fbi.gov/news/stories/two-from-syrian-electronic-army-added-to-cybers-most-wanted

Fowler, Sarah. 2013. "Who is the Syrian Electronic Army?" BBC, April 25, 2013. https://www.bbc.com/news/world-middle-east-22287326

Norman, Helmi. 2019. "The emergence of open and organized pro-government cyber attacks in the Middle East: The case of the Syrian Electronic Army." *OpenNet Initiative*. https://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army

Smith-Spark, Laura. 2013. "What is the Syrian Electronic Army?" CNN, August 28, 2013. https://www.cnn.com/2013/08/28/tech/syrian-electronic-army/index.html

Stracqualursi, Veronica, and Adam Kelsey. 2017. "The rise of Syria's controversial president Bashar al-Assad." *ABC News*, April 7, 2017. https://abcnews.go.com/Politics/rise-syrias-controversial-president-bashar-al-assad/story?id=46649146

United States Department of Justice. 2016. "Syrian Electronic Army hacker pleads guilty." September 28, 2016. https://www.justice.gov/opa/pr/syrian-electronic-army-hacker-pleads-guilty

Weiner, Rachel. 2018. "Two hackers accused of tricking reporters indicted." *Washington Post*, May 17, 2018. https://www.washingtonpost.com/local/public-safety/syrian-hackers-who-allegedly-tricked-reporters-indicted/2018/05/17/069ef328-59e7-11e8-858f-12becb4d6067_story.html?utm_term=.420c64641c92

T

TEAMPOISON

TeaMpoisoN was a hacking group found in Britain whose teenaged members have hacked into the North Atlantic Treaty Organization (NATO), Facebook, and the English Defense League, as well as former UK Prime Minister Tony Blair's e-mail. The members have previously worked alongside other notorious hackers from the group Anonymous to launch an assault on banks under the codename "Operation Robin Hood."

In an early hack, the members gained access to the United Nations computers and posted the e-mails, login information, and passwords for the organization online. According to the UN, the group posted information on over 100 individuals who worked in the Development Program (UNDP), the Organization for Economic Cooperation and Development (OECD), UNICEP, the World Health Organization (WHO), and other groups.

In 2010, members of TeaMpoisoN were able to hack into Facebook and post unauthorized status updates onto hundreds of pages, including those belonging to Mark Zuckerberg and the president of France, Nicolas Sarkozy. They team members also leaked personal information pertaining to the leadership of the English Defence League. It has been alleged that members of TeaMpoisoN have worked with members of Anonymous to carry out an attack on banks, calling it "Operation Robin Hood."

In 2012, a TeaMpoisoN member Junaid Hussain pleaded guilty in London to hacking into the web server belonging to former U.K. Prime Minister Tony Blair, and then posting the e-mail addresses, phone numbers, and postal addresses for Blair's family. He also posted the contact information for members of parliament. Hussain called himself "Trick." He joined the group before he graduated from high school. Many years later, Hussain joined the terrorist organization ISIS as a hacker to carry out cyberattacks. He quickly became the third highest–ranked ISIS member on the Pentagon's kill list. It was reported that he was killed as part of a U.S. drone strike.

That same year, law enforcement in Newcastle (England) arrested a 17-year-old whom they suspected of belonging to TeaMPoisoN after the group was linked to over 1,000 incidents of hacking, including a hack into the phone systems of the counterterrorism unit at Scotland Yard and an attack on the website of the United Kingdom's Serious Organised Crime Agency (SOCA). This member went by the name MLT. He was charged with violating the Computer Misuse Act and faced up to ten years in prison.

After MLT was arrested, TeaMpoisoN disbanded. MLT emerged as a white-hat security expert, giving his attention to legal computer security endeavors such as identifying vulnerabilities in different websites, including the U.S. Department of Defense. He also founded a computer security research organization called Project Insecurity that teaches individuals about security awareness.

In 2015, it was reported that Hussain was killed by a U.S. drone strike near Raqq, Syria. Since his early days in TeaMpoisoN, Hussain had become a top member of the terrorist group the Islamic State of Iraq and Syria. Law enforcement also thought that he had become the leader of the CyberCaliphate hacking group that had been blamed for spreading propaganda by defacing websites and hacking into social media accounts.

See also: Anonymous; Hacker and Hacking

Further Reading

Albanesius, Chloe. 2011. "Team Poison hacks UN, leaks usernames, passwords." *PCMag*, November 30, 2011. https://www.pcmag.com/article2/0,2817,2397032,00.asp

Ashford, Warwick. 2012. "Police arrest suspected Team Poison hacker." *Computer Weekly*, May 11, 2012. https://www.computerweekly.com/news/2240150117/Police-arrest-suspected-TeamPoison-hacker

Cluley, Graham. 2015. "Team Poison hacker believed killed by U.S. drone strike." Bitdefender, August 28, 2015. https://hotforsecurity.bitdefender.com/blog/team-poison-hacker-believed-killed-by-us-drone-strike-12576.html

Franceschi-Bicchierai, Lorenzo. 2015. "How a teenage hacker became the target of a U.S. drone strike." *Vice*, August 28, 2015. https://www.vice.com/en_us/article/jp5wed/junaid-hussain-isis-hacker-drone

Furness, Hannah. 2012. "Team Poison: Profile of the hackers." *The Telegraph*, April 12, 2012. https://www.telegraph.co.uk/technology/9200751/Team-Poison-profile-of-the-hackers.html

Paletta, Damian, Danny Yadron, and Margaret Coker. 2015. "World news: U.S. drone strike kills a top hacker for Islamic State." *Wall Street Journal*, August 27, 2015. https://www.wsj.com/articles/u-s-drone-strike-kills-islamic-statehacker-1440643549

TOOLS

A cybercrime tool is any item that assists a cybercriminal in their perpetration of cybercrimes. Cybercrime tools fall generally into two categories: software and hardware. Software tools are programs that are designed to either carry out a specific cybercrime purpose or are used in such a fashion. Computer viruses and ransomware are examples of software that is specifically designed to enable the commission of cybercrime. Viruses are designed to replicate themselves on an infected computer and cause harm, whether that be the theft of personally identifying information, or the deletion of important files. Ransomware is designed to lock a user out of their computer until the cybercriminal behind the ransomware attack is paid off by the victim. Other software may have a legitimate use, but cybercriminals can use the software for criminal purposes. A sniffer would be an example of this. A sniffer is software that allows someone to see and record the data travelling across a computer network. A sniffer can be used for legal purposes, such as diagnosing connectivity issues, recovering forgotten login credentials, and analyzing network traffic (Ansari et al., 2003). However, cybercriminals can use a sniffer to commit cybercrimes, such as intercepting and stealing personally identifying information being transmitted across a computer network.

Cybercriminals also use hardware tools. A hardware tool would be a physical device used by a cybercriminal to commit cybercrime. Perhaps the most basic hardware tool would be a computer or other similar electronic device. In order to run software tools, a cybercriminal will need to have one of these devices. These are not the only cybercrime hardware tools, however. An example of another hardware tool would be a skimmer, which is a physical device that is placed over a legitimate payment card slot, such as a credit card slot on a gas pump or at an ATM machine. The device is able to detect and copy the information from a payment card. A cybercriminal can use that information to commit credit card fraud.

There are some cybercrime tools that can be either software or hardware. An example of this would be a pen register. A pen register is a physical device that keeps a log of the telephone numbers that are called from a phone line. There is software that replicates this same functionality, and it would also be referred to generally as a pen register. Another example is a keystroke monitor—software that keeps a log of the keys pressed on a keyboard. These are used to capture and steal the personally identifying information of those using the keyboard. While not necessarily referred to as keystroke monitors, there are physical devices that perform a similar function. Some cybercriminals who use skimmers use a keypad plate that goes over the top of a keypad on an ATM machine or similar device. The keypad is designed to not only keep a log of the buttons pushed but also to trigger the buttons under them. This allows a victim to complete a transaction at an ATM machine without being aware that their PIN number has been stolen (Federal Deposit Insurance Corporation, 2018).

Other cybercrime tools are a combination of software and hardware. An example of this would be a botnet. A botnet is a network of computer that have been infected with malware that permits a cybercriminal to surreptitiously control those computers. The malware component of a botnet is software, but a botnet does not work without infected computers, which would be hardware.

Over time, the cost of some cybercrime tools has decreased. Malware that can be used to steal personally identifying information has become less expensive. There are some cybercrime activities that have become purchasable as a service, making it more affordable to a wider array of potential cybercriminals. An example of this is organizations that have existing botnets in place to distribute spam. Someone can pay one of these organizations to distribute spam via that botnet instead of having to establish their own botnet to distribute spam. The cost for this can be relatively cheap, with one organization offering to distribute a million spam e-mails for $200, and some Russian websites offering similar services for as low as $10 (Barbaschow, 2017; Goncharov, 2012).

See also: Bots and Botnets; Credit Card Fraud; Keystroke Monitoring; Pen Register; Personally Identifying Information; Malware; Ransomware; Skimmer; Sniffer; Spam; Tor (The Onion Router); Virus; War Dialer

Further Reading

Ansari, Sabeel, S.G. Rajeev, and H.S. Chandrashekar. 2003. "Packet sniffing: A brief introduction." *IEEE Potentials* 21, 5: 17–19.

Barbaschow, Asha. 2017, September 19. "Low-cost tools making cybercrime more accessible: SecureWorks." *ZDNet*. https://www.zdnet.com/article/low-cost-tools-making-cybercrime-more-accessible-secureworks/

Federal Deposit Insurance Corporation. 2018. "Beware of ATM, debit and credit card 'skimming' schemes." https://www.fdic.gov/consumers/consumer/news/cnwin18/cardskimming.html

Goncharov, Max. 2012. "Russian underground 101." Trend micro incorporated. https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

TOR (THE ONION ROUTER)

Tor (an acronym for "The Onion Router") is software that allows users to navigate the internet in a more anonymous capacity. The initial version of the software was released in 2002. Tor increases anonymity of users by utilizing a network of computers (nodes). The Tor software picks a random path of nodes to go through when a user accesses a server, the links between each node being encrypted. By doing this, the origin of the user's computer is obfuscated (Tor, 2018).

Tor software can be used for many legitimate purposes. As the developers of the software note, it can be used by journalists to communicate with whistleblowers, the military to gather intelligence, and individuals who simply wish to conduct a sensitive search of the internet anonymously (Tor, 2018). Indeed, the vast majority of web traffic through Tor appears to be for legitimate purposes (Greenberg, 2015).

Though the majority of web traffic through Tor is legitimate, there is a fair amount that is not. The Tor software not only allows users to navigate the internet anonymously, it also allows users to host websites anonymously. These are known as Tor hidden services (Greenberg, 2015). Collectively, the hidden service sites that are accessible through Tor and similar services are known as the dark web. It appears the Tor hidden services are commonly used for conducting criminal activity, such as drug trafficking, money laundering, and distribution of child pornography (Greenburg, 2015; Moore and Rid, 2016). Indeed, Silk Road—an online marketplace that was known for drug sales—was a Tor hidden service.

The U.S. government has had a hand in the development of Tor. Tor originally was developed by the Office of Naval Research starting in 1995 (Onion Routing, 2005). Its goal was to protect government communications (Tor, 2019). The project was handed over to Roger Dingledine and Nick Mathewson—both programmers—in 2002 (Zetter, 2005). The government continues to use Tor for intelligence gathering and to protect the online activity of military agents (Tor, 2019). The ability of Tor to provide privacy and security to the online activity of its users increases the more users it has. This is so because the more users there are, the less likely it becomes that a third party monitoring web traffic will be able to determine who it sending data. It appears this may have been part of the reason the Office of Naval Research turned the project over in the first place—to diversify the user base of Tor so those monitoring Tor traffic would not easily deduce that Tor web traffic likely originated from the navy (see Zetter, 2005). The U.S. government has continued funding the development of Tor over the years. There appears to be some evidence that the developers of Tor would notify the U.S. government of vulnerabilities Tor faced before it notified all its users (Farquhar, 2018).

See also: Dark Web; Privacy; Silk Road; Snowden, Edward

Further Reading

Farquhar, Peter. 2018, March 2. "An FOI request has revealed 'anonymous' browser Tor is funded by U.S. government agencies." *Business Insider Australia*. Retrieved from https://www.businessinsider.com.au/claims-tor-funded-by-us-government-agencies-2018-3 on October 30, 2018.

Greenberg, Andy. 2015, January 28. "No, Department of Justice, 80 percent of tor traffic is not child porn." *Wired*. https://www.wired.com/2015/01/department-justice-80-percent-tor-traffic-child-porn/

Moore, Daniel, and Thomas Rid. 2016. "Cryptopolitik and the Darknet." *Survival* 58: 7–38.

Onion Routing. 2005. "Brief selected history." https://www.onion-router.net/History.html

Tor. 2018. "Tor: Overview." https://www.torproject.org/about/overview.html.en

Tor. 2019. "Inception." https://www.torproject.org/about/torusers.html.en

Zetter, Kim. 2005, May 17. "Tor torches online tracking." *Wired*. https://www.wired.com/2005/05/tor-torches-online-tracking/?currentPage=all

TROJAN HORSE

The Trojan horse comes from Greek mythology. During the Trojan War, the Greeks were at war with the inhabitants of the city of Troy. The Greeks came up with a ploy to conquer the city. The Greeks built a large wooden horse that was hollow. Greek soldiers hid inside the horse. The remainder of the Greek army pretended to leave, and the horse was left for the inhabitants of Troy as a supposed gift. The horse was brought into Troy. The Greek soldiers exited the horse at night and conquered the city of Troy.

The term "Trojan horse" has been used to describe malware that operates in the same way the Trojan horse operated against Troy. It appears the term was first used in reference to certain types of malware in a U.S. military report from 1974 (Karger and Schell, 1974). A Trojan horse program is first intentionally installed on a computer by a victim, with the victim being unaware of one or more malicious functions that program is capable of carrying out. This is often accomplished through some sort of deception, just as the original Trojan horse was brought into Troy through deception. For example, someone might download a helpful piece of freeware from the internet, but the freeware might contain a harmful payload that can be subsequently released on the victim's computer.

Beyond this, it is not exactly clear what separates a Trojan horse from other forms of malware. Trojan horses—as well as several other forms of malware—have been defined in several different ways, with various classification schemes designed to differentiate these forms of malware (see Karresand, 2002). In particular, how a Trojan horse differs from a virus or a worm has not been definitively resolved. Some see Trojan horses as a subclass of viruses, whereas others see it the other way around with viruses being a subclass of Trojan horses. Others see some overlap between Trojan horses and worms as well (see Karresand, 2002).

While exact definitions may vary, the key aspect that appears to make a Trojan horse a Trojan horse is the element of deception. If deception is used to induce a victim to download malware to his or her computer, that malware would be considered a Trojan horse. Software that is downloaded that performs functions that are not authorized by the victim could also be considered a Trojan horse (see Karresand, 2002). For example, a piece of freeware (such as a web browser) may not do any affirmative damage to a victim's computer nor steal a victim's personal information, but it may track the victim's web usage habits for commercial purposes. If the victim is not made aware this will be done by the freeware, the freeware could be viewed as a Trojan horse. If the victim is made aware this will be done (such as through an end user agreement), then the victim has not been deceived and the freeware would not be considered a Trojan horse.

See also: Malware; Payload; Virus; Worm

Further Reading

Karger, Paul A., and Roger R. Schell. 1974. *Multics security evaluation: Vulnerability analysis*. Hanscom AFB, MA: Electronic Systems Division.

Karresand, Martin. 2002. *A proposed taxonomy of software weapons*. Master's thesis in Computer Security at Linköping University, Sweden.

U

UBER HACK

Uber is a ridesharing service that requires customers provide the company with their payment information (credit card) prior to the ride, which is then stored by the company for future use through the Uber mobile app. Drivers are required to provide Uber with their name, e-mail, phone number, address, government identification number (social security number, driver's license or passport number), birthday, photo and signature. They must also provide information about their vehicle and insurance. Uber also looks at a driver's background information, such as their driving history or criminal background. Those using the service must provide their location, the type of service requested, the date and time of the service, the amount charged, distance traveled, and payment method (Uber, 2018). The company suffered two cyberattacks, first in May 2014, and again in 2016. The attacks stole personal information of approximately 1 million Uber drivers and 57 million Uber riders. The company failed to quickly disclose that it had been the victim of cyberattacks, angering many customers whose personal information may have been compromised. The company was eventually fined $148 million for their lack of action.

In May 2014, Uber's computer systems were hacked and the personal information of an estimated 1 million former and current drivers was stolen (a number originally estimated to be only 50,000). This included not only the names and license plate numbers of the drivers but also bank account information and routing numbers. Company officials did not report this hack quickly, waiting until eight months after it was discovered to announce it.

Then, in 2016, two hackers gained unauthorized access to the company's computer system and stole personal data, including home and cell phone numbers, e-mail addresses, and names of up to 57 million Uber users. They also stole 600,000 driver's license numbers of the company's drivers. No Social Security numbers, credit card information, or details about the rides were accessed. The hackers did not access the corporate computer systems or infrastructure. This time, Uber officials waited until November 2017, to announce that the company had been hacked.

The stolen data had been stored on an Amazon Web Services cloud account. The company paid the hackers $100,000 so they would not release the stolen data, a common practice by businesses. However, Uber officials did not inform the potential victims or regulators, as required by law. The hackers reportedly destroyed the data they stole.

Many people, especially those who lost data, accused Uber officials of covering up the attack. The CEO of the company, Dara Khosrowshahi, reported that he would investigate the delay and possible coverup, but did announce that the two people who were responsible for hiding the breach had been released from their positions and were no longer employed by the company. This included the chief security officer Joe Sullivan and Craig Clark, the legal director of security and law enforcement. He also reported that the company would increase its security measures to ensure that no additional breaches would occur. In an additional gesture of good will to the victims, the company offered to provide free identity theft protection and credit monitoring for any of the drivers whose license numbers were stolen in the breach. Despite this good will from the company, critics of Uber were vocal. Sam Curry, chief security officer for a computer security firm Cybereason said, "The truly scary thing here is that Uber paid a bribe, essentially a ransom to make this breach go away, and they acted as if they were above the law" (Liedtke, 2017).

In a statement made to the public, Khosrowshahi e-mailed, "None of this should have happened, and I will not make excuses for it. . . . We are changing the way we do business" (Khosrowshahi, 2017).

To date, there have been no indications of any fraud resulting from the breach, but Vice Motherboard reported that the stolen account information was available for sale on the dark web for between $1 and $5 (Cox, 2015).

See also: Ashley Madison Breach; Ransomware; Reputation, Effects on

Further Reading

Brewster, Thomas. 2017. "FTC: Uber failed to protect 100,000 drivers in 2014 hack." *Forbes*, August 15, 2017. https://www.forbes.com/sites/thomasbrewster/2017/08/15/uber-settles-ftc-complaint-over-secuirty-and-privacy/#61e1b92588da

Cox, Joseph. 2015. "Stolen Uber customer accounts are for sale on the dark web for $1." *Vice Motherboard*, March 27, 2015. https://www.vice.com/en_us/article/z4mk7j/stolen-uber-customer-accounts-are-for-sale-on-the-dark-web-for-1

Griswold, Alison. 2015. "Looks like Uber got hacked." *Slate*, February 27, 2015. https://slate.com/business/2015/02/uber-hack-50000-drivers-may-be-affected-in-2014-security-breach.html

Khosrowshahi, Dara. 2017. "2016 data security incident." *Uber Newsroom*, November 21, 2017. https://www.uber.com/newsroom/2016-data-incident/

Larson, Selena. 2017a. "Uber hack in 2016 expose data on 57 million people." *CNN*, November 22, 2017. http://money.cnn.com/2017/11/21/technology/uber-hacked-2016/index.html

Larson, Selena. 2017b. "Uber's massive hack: What we know." *CNN Business*, November 23, 2017. https://money.cnn.com/2017/11/22/technology/uber-hack-consequences-cover-up/index.html

Liedtke, Michael. 2017. "Uber reveals cover-up of hack affecting 57M riders, drivers." Associated Press, November 22, 2017. https://www.apnews.com/b0f1c1d3b44849be9a4640264d28e44c

Newcomer, Eric. 2017. "Uber paid hackers to delete stolen data on 57 million people." *Bloomberg*, November 21, 2017. https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data

Uber. 2018. "Privacy Policy." https://privacy.uber.com/policy/

UNION DIME SAVINGS BANK THEFT

Union Dime Savings Bank was situated in New York City. In the early 1970s, one of the bank's supervisors, Roswell Steffen, was arrested for stealing roughly $1.5 million. The theft was sizable for a savings bank at the time. It was also one of the first instances of a bank thief using a computer to accomplish the theft.

Steffen would remove several thousand dollars from various accounts. When it came time for interest payments to be made to these accounts, Steffen would redeposit the funds and then draw those funds back out after the interest payments were made. With every fraudulent transaction, Steffen would adjust the numbers in the computerized accounts to make everything appear normal. By doing this, Steffen avoided detection for some time (see Fosburgh, 1973). It appears that some of these abnormal transactions had been detected by auditors and others at the bank. However, it seems that no follow-up investigation was ever conducted by the bank (see EDP Audit, Control, and Security Newsletter, 1975).

The theft was ultimately discovered as part of an entirely different investigation. Steffen was using the money he embezzled to gamble. The bookmaking organization with which Steffen placed his bets was being investigated. Investigators noticed that Steffen was placing sizeable bets on a daily basis—at least $30,000. This drew their attention, and they looked into Steffen's situation further. They discovered that the amount of money Steffen was gambling greatly exceeded his annual income. This ultimately led to an investigation into Steffen's behavior at work and the discovery of the theft of $1.5 million from accounts there (Fosburgh, 1973).

This case does illustrate some interesting points about cybercrime. Cybercrime does not have to involve complex schemes, knowledge of how to hack a network, and so forth. In this case, Steffen was an employee of the bank—and a supervisor at that. He had permission to access the computer network and log transactions. He simply falsified those transactions. It appears there were some procedures in the bank to detect falsified transactions, but lack of follow-up on suspicious transactions discovered following those procedures ultimately resulted in a failure to detect the theft. This same thing can happen today. Computer networks can be protected by firewalls and other measures, but there is always a human element required for network security (e.g., a system administrator, IT department). If one of those humans decides to either compromise the security of that network or allow that security to be compromised by someone else, then those security measures can be easily bypassed. Thus, no matter how advanced a network's security software and hardware is, it is still important to have measures in place to ensure that an organization's employees are not negating that security.

See also: Financial Crimes; Fraud

Further Reading

EDP Audit, Control, and Security Newsletter. 1975. "Abstracts & commentaries." *EDP Audit, Control, and Security Newsletter* 3, 4: 14–19.

Fosburgh, Lacey. 1973, March 23. "Chief Teller is accused of theft of $1.5-million at a bank here." *New York Times*, p. 1. https://www.nytimes.com/1973/03/23/archives/chief-teller-is-accused-of-theft-of-15million-at-a-bank-here-teller.html

UNITED LOAN GUNMEN

The United Loan Gunmen was a hacker group the carried out a string of attacks on prominent websites in 1999. This included ABC, C-Span, the Drudge Report, NASDAQ, and the Associated Press. The attacks generally consisted of cybervandalism, with the group editing the home page of the sites they attacked.

With the ABC website, the group posted a message apparently protesting the encroachment of media companies into the internet. A portion of the message read: "As what has always happened [sic] with television, radio, and newspapers, corporations and companies are trying to stake there [sic] claim into our information superhighway. Unlike the world of TV and radio . . . the common man, like you and I, can take control" (Glave, 1999a).

A few weeks after the attack on ABC, C-Span was hit. The group posted a fabricated transcript of a conversation between the U.S. Secretary of War (a position that does not exist) and the leader of a country in the Middle East that took place in 1983. The transcript claimed that the United States was planning on starting a conflict in the Middle East to benefit the U.S. military industrial complex (Associated Press, 1999b).

Roughly a week after the C-Span attack, the Drudge Report website—a media website that at the time of the attack tended to focus on gossip—was attacked. While not known for certain, it is possible the site was targeted after Matt Drudge—the namesake of the site—mentioned the United Loan Gunmen during his radio news program. The group left the following message: "United Loan Gunmen take control of Matt Drudge's Data Stockyard to once again show the world that this is the realm of the hacker." They also added news headlines to the site. Notably, they added the headline "Kevin Mitnick Still in Jail," with the headline linking to a website seeking Mitnick's release (Glave, 1999b). Mitnick was a prominent hacker who was serving time in prison at the time of this attack.

Just days after the attack on the Drudge Report, the group attacked NASDAQ. This attack broke the pattern of previous attacks carried out by the group. The previous attacks had targeted the websites of media outlets. This attack target a significant financial institution. Again, it appears the group just left a message on the home page of NASDAQ's website. The message read: "The Elite Computer Hacking group ULG uprooted the Nasdaq Stock Market Web Site. . . . Their goal was to attempt to make stocks rise drastically, thus making all investors happy, hopefully ending with the investors putting bumper stickers on their Mercedez [sic] that say 'Thanks ULG!'" (Kahney, 1999).

Over a month later on Halloween, the group again targeted a media outlet and attacked the Associated Press. The message in this attack was simply an Edgar Allan Poe poem (Associated Press, 1999a).

There has been some speculation that the United Loan Gunmen may have been the same group as Hacking for Girlies—another hacker group at the time (Burrough, 2000; Kahney, 1999). Hacking for Girlies was responsible for an attack on the New York Times's website roughly a year prior to the attacks carried out by the United Loan Gunmen. Similarities between the attack on the *New York Times* and the attacks by the United Loan Gunmen have been noted—such as the code used by both groups. However, there is no definitive proof that the two groups are one and the same (Burrough, 2000).

See also: Hacker and Hacking; Vandalism

Further Reading

Associated Press. 1999a. "Hackers break in to AP web site." *Washington Post*, October 31, 1999. http://www.washingtonpost.com/wp-srv/aponline/19991031/aponline164929_000.htm

Associated Press. 1999b. "Hackers vandalize C-Span web site." *AP Online*. EBSCOhost, September 6, 1999. search.ebscohost.com/login.aspx?direct=true&db=n5h&AN=861a564324e6982d1f719e7e4b049aa1&site=eds-live

Burrough, Bryan. 2000. "Invisible enemies." *Vanity Fair*, June 2000. https://www.vanityfair.com/news/2000/06/web-hackers-200006

Glave, James. 1999a. "ABC site falls to crackers." *Wired*, August 20, 1999. https://www.wired.com/1999/08/abc-site-falls-to-crackers/

Glave, James. 1999b. "Foes with grudge sludge drudge." *Wired*, September 14, 1999. https://www.wired.com/1999/09/foes-with-grudge-sludge-drudge/

Kahney, Leander. 1999. "Latest cracker caper: NASDAQ." *Wired*, September 15, 1999. https://www.wired.com/1999/09/latest-cracker-caper-nasdaq/

UNITED STATES CYBER COMMAND

The United States Cyber Command is the 10th Unified Combatant Command in the United States. A Unified Combatant Command is a joint military command (i.e., at least two branches of the military are involved in the command) with wide-ranging missions that are overseen by a single commander (Joint Chiefs of Staff). Those commands may oversee a specific geographic area, or—as in the case of Cyber Command—it may oversee a specific content area.

As a unit of the U.S. military, Cyber Command's focus is primarily on cyber wrongdoing as a warfare matter. In this aspect, it differs from other federal agencies like the FBI, ICE, and the Secret Service, who are not part of the military and focus on cyber wrongdoing as a criminal matter. There are cyberattacks that could be handled as both a criminal matter and a military matter. For example, in 2016, cybercriminals launched a cyberattack against a U.S. water system, hitting the computers that regulated the chemical levels in the water supply. The cybercriminals are believed to have ties to Syria (Mahairas and Beshar, 2018). The attack on the water system would be a crime. However, where U.S. infrastructure was also targeted, the attack arguably falls under the ambit of Cyber Command's mission. Thus, while Cyber Command does primarily focus on the military aspect of cyber wrongdoing, there are occasions where it can assist in cybercrime matters (see U.S. Cyber Command, 2018).

Cyber Command is located at Fort Meade, Maryland. It became a Unified Combatant Command on August 18, 2017. Cyber Command did exist prior to this as a subunified command under Strategic Command (another Unified Combatant Command) as of November 12, 2008 (U.S. Cyber Command, 2019). The mission of Cyber Command is to “direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and foreign partners” (U.S. Cyber Command, 2018). As part of this mission, Cyber Command does work to defend U.S. Department of Defense computer systems from cyberattack. Additionally, it works to defend the U.S. infrastructure from cyberattacks in general (U.S. Department of Defense, 2018).

There are numerous entities that can launch cyberattacks against the United States. As noted above, cybercriminals can launch such attacks. Terrorist organizations or hacktivist groups may do the same (U.S. Cyber Command, 2018). While Cyber Command does work to prevent cyberattacks from all sources, its focus is on cyberattacks from countries (Department of Defense, 2018).

See also: Federal Bureau of Investigation; Hacktivism; Immigration and Customs Enforcement; Secret Service

Further Reading

Joint Chiefs of Staff. 2017. “Joint Publication 1, Doctrine for the Armed Forces of the United States.” Joint Chiefs of Staff, July 12, 2017. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf

Mahairas, Ari, and Peter J. Beshar. 2018. “A perfect target for cybercriminals.” *The New York Times*, November 19, 2018. https://www.nytimes.com/2018/11/19/opinion/water-security-vulnerability-hacking.html

U.S. Cyber Command. 2018. “Achieve and maintain cyberspace superiority: Command vision for US cyber command.” https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

U.S. Cyber Command. 2019. “U.S. cyber command history.” https://www.cybercom.mil/About/History/

U.S. Department of Defense. 2018. “Department of defense cyber strategy.” https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

UNLIMITED OPERATION

An unlimited operation is a cyberattack used to potentially withdraw an unlimited amount of money from numerous ATMs. To accomplish this, cybercriminals must first have access to the payment card information (credit card, debit card, prepaid card, ATM card, etc.) of the account they wish to deplete. This information can be obtained from victims through a phishing attack, through the use of malware (such as keystroke monitor) or through the use of hardware such as a skimmer (Federal Financial Institutions Examination Council, 2014; Frazee, 2018). Once cybercriminals have this information, they use malware to remove the withdrawal limits placed on the payment card. Cybercriminals will also adjust or disable security measures put in place to alert the bank and victims of potential fraudulent use of their card. Next, the card information is distributed to numerous other cybercriminals at different locations. Those cybercriminals will then execute a simultaneous attack at ATMs in those different locations. With the withdrawal limits removed, the cybercriminals are able to withdraw an "unlimited" amount of money from ATMs (limited only by the amount of money actually in the ATMs targeted). Money is withdrawn until financial institutions recognize what is going on and prevent further withdrawals (Federal Financial Institutions Examination Council, 2014; United States Attorney's Office Eastern District of New York, 2014).

The amount of money that can be stolen through this method is substantial. In 2011, an international cybercriminal organization managed to steal $14 million in just 48 hours. In that instance, the organization obtained prepaid debit card information to perpetrate the unlimited operation. The prepaid debit cards were ones that the American Red Cross intended to provide to disaster victims. Qendrim Dobruna—one of the members of that cybercriminal organization—pleaded guilty to bank fraud and was sentenced to 50 months in prison in 2015 (United States Attorney's Office Eastern District of New York, 2014, 2015). In 2012 and 2013, another international cybercriminal organization carried out two unlimited operation attacks, stealing a combined total of $45 million. In the first attack, the organization targeted a company that processed prepaid debit cards in the United Arab Emirates. The second attack targeted a similar company is Oman. In the United States, seven members of this cybercriminal organization were arrested for their involvement in these attacks—Jael Mejia Collado, Joan Luis Minier Lara, Evan Jose Pena, Jose Familia Reyes, Elvis Rafael Rodriguez, Emir Yasser Yeje, and Chung Yu-Holguin (United States Attorney's Office Eastern District of New York, 2013).

As with cybercrime in general, there is the risk that another unlimited operation attack could be carried out. Indeed, in late 2018, the Federal Bureau of Investigation (FBI) provided a warning to financial institutions concerning an imminent unlimited operation attack. It appears the warning may have been in relation to an unlimited operation attack that happened shortly after the warning was given. In that incident, approximately $13.5 million was stolen from accounts through an Indian bank in India, Hong Kong, and Canada (Krebs, 2018).

See also: Credit Card Fraud; Federal Bureau of Investigation; Keystroke Monitoring; Malware; Phishing; Skimmer

Further Reading

Federal Financial Institutions Examination Council. 2014. "Cyber-attacks on financial institutions' ATM and card authorization systems." April 2, 2014. https://ithandbook.ffiec.gov/media/154261/unlimited_atm_cash-out_4-2-2014-final.pdf

Frazee, Gretchen. 2018. "Hackers are preparing an 'unlimited' ATM cash heist. Here's how to protect yourself." *PBS*, August 15, 2018. https://www.pbs.org/newshour/economy/hackers-are-preparing-an-unlimited-atm-cash-heist-heres-how-to-protect-yourself

Krebs, Brian. 2018. "FBI warns of 'unlimited' ATM cashout blitz." Krebsonsecurity, August 12, 2018. https://krebsonsecurity.com/2018/08/fbi-warns-of-unlimited-atm-cashout-blitz/

United States Attorney's Office Eastern District of New York. 2013. "Eight members of New York cell of cybercrime organization indicted in $45 million cybercrime campaign." United States Department of Justice, May 9, 2013. https://www.justice.gov

/usao-edny/pr/eight-members-new-york-cell-cybercrime-organization-indicted-45-million-cybercrime#FOOT1

United States Attorney's Office Eastern District of New York. 2014. "International hacker pleads guilty to 2011 global cyberattack." United States Department of Justice, July 11, 2014. https://www.justice.gov/usao-edny/pr/international-hacker-pleads-guilty-2011-global-cyberattack

United States Attorney's Office Eastern District of New York. 2015. "Cybercriminal sentenced to 50 months for his role in hacking campaign." United States Department of Justice, June 29, 2015. https://www.justice.gov/usao-edny/pr/cybercriminal-sentenced-50-months-his-role-hacking-campaign

U.S. PRESIDENTIAL ELECTION INTERFERENCE, 2016

During the 2016 U.S. presidential election, Russia used cyberattacks in an attempt to influence the election's outcome. According to Robert S. Mueller (2019)—the special counsel appointed to investigate Russia's interference in the election—Russia's interference had a two-prong approach. First, Russia engaged in a misinformation campaign using false social media accounts. Second, Russia infiltrated the computers of individuals and other entities associated with the campaign of presidential candidate Hilary Clinton, stole information from those computers, and then released that information to the public.

The misinformation campaign conducted by Russia was done through the IRA. The IRA is a Russian organization funded by Russian oligarch Yevgeniy Viktorovich Prigozhin. Prigozhin is believed to have ties to Vladimir Putin, the president of Russia. Members of the IRA created false social media accounts, pretending to be activists in the United States. The accounts would occasionally falsely claim that the fictitious activist was affiliated with an actual political organization in the United States. These accounts would be used to spread information with the purpose of influencing the United States electorate. The IRA started in 2014. Its initial goal was to create discord generally in the political system of the United States. By 2016, the goal of the IRA became more specific. The information it spread was designed to favor presidential candidate Donald Trump and discredit Hilary Clinton. It is believed that this shift in goals occurred—at least in part—because Putin blamed Clinton for inciting protests against him in 2011 and 2012 while she was secretary of state (Office of the Director of National Intelligence, 2017). The IRA was able to reach a sizeable portion of the electorate through their efforts. Facebook estimated the IRA was able to reach approximately 126 million people through its accounts on the social media platform. Twitter estimated that over a million of its users had been reached by IRA accounts on its platform. In some instances, political figures in the United States had retweeted information from IRA Twitter accounts (albeit without knowledge that the accounts were IRA-run). In addition to false accounts, the IRA also paid for advertisements on Facebook to try and reach and influence more people. Facebook indicated the IRA had purchased over 3,500 advertisements.

Russian efforts to hack into computers and other databases of those associated with the Clinton campaign began in 2016. These attacks were carried out by Russia's GRU. Among those hit were Clinton's campaign chairman John Podesta and the Democratic National Committee. The GRU used spearphishing to gain access to the e-mail accounts of victims. Information gained from the e-mail accounts of victims of the spearphishing was used to access the networks of other victims. Among the documents stolen were personal e-mails, fundraising data, and opposition research on Trump. The documents were released to the public prior to the election through online entities created by the GRU, known online as "DCLeaks" and "Guccifer 2.0." WikiLeaks also released some of these documents (WikiLeaks, 2016). Evidence exists that indicates the documents were sent to WikiLeaks by the GRU, though WikiLeaks denies it received the documents from Russia. WikiLeaks appears to have gotten involved due to Julian Assange's opposition to Clinton. This incident led to accusations against WikiLeaks of being biased and politically motivated (Smith, 2016). The timing of the releases by WikiLeaks seemed to further such opinions. For example, speeches Clinton gave to Wall Street bankers—wherein she expressed that it was necessary in politics to have "both a public and a private position" (BBC News, 2016)—were released minutes after video surfaced of Trump bragging about groping women (Smith, 2016).

Mueller's investigation into Russia's interference in the 2016 presidential election resulted in the indictment of 25 Russian individuals and three Russian companies. Of those 25 individuals, 12 were officers in the GRU. The companies charged include the IRA and two shell companies that were used to fund the IRA. Among the individuals indicted is Prigozhin, the financier of the IRA (Prokop, 2019).

While the results of Mueller's investigation provide evidence of Russia's interference in the 2016 presidential election in the United States, not everyone has agreed that this is the case. Russia has denied that it interfered. Also, Trump has discounted Russia's involvement in the 2016 election, casting such claims as a fiction concocted by supporters of Clinton to explain why she lost the election (Decker, 2016).

Russia's interference in the 2016 presidential election does not appear to be an isolated incident. Russia also attempted to influence the United States electorate during the 2018 midterm elections (Ferran and Good, 2018). One Russian citizen—Elena Khusyaynova—was indicted for conspiring to defraud the United States by spending over $10 million on political advertisements in the United States for the purpose of interfering with the political system in the United States. It is believed that Khusyaynova works for Concord—one of the shell companies used to fund the IRA that was indicted by Mueller (Gerstein, 2018).

See also: Assange, Julian; Phishing; Russia; Social Media; WikiLeaks

Further Reading

BBC News. 2016. "18 revelations from Wikileaks' hacked Clinton emails." October 27, 2016. https://www.bbc.com/news/world-us-canada-37639370

Decker, Cathleen. 2016. "Russian hacking controversy is the fault of Hillary Clinton supporters and politics, Donald Trump and his team say." *The L.A. Times*, December 12, 2016. https://www.latimes.com/nation/politics/trailguide/la-na-trailguide-updates-hillary-clinton-and-politics-are-to-1481564624-htmlstory.html

Ferran, Lee, and Chris Good. 2018. "No evidence of midterm vote tampering, but influence operations persisted: US intelligence." *ABC News*, December 22, 2018. https://abcnews.go.com/Politics/evidence-midterm-vote-tampering-influence-operations-persisted-us/story?id=59964734

Gerstein, Peter. 2018. "U.S. brings first charge for meddling in 2018 midterm elections." *Politico*, October 19, 2018. https://www.politico.com/story/2018/10/19/first-criminal-case-filed-over-russian-interference-in-2018-midterms-916787

Mueller, Robert S. 2019. "Report on the investigation into Russian interference in the 2016 presidential election." Volume 1. United States Department of Justice. https://www.justice.gov/storage/report.pdf

Office of the Director of National Intelligence. 2017. "Background to 'Assessing Russian activities and intentions in recent US elections': The analytic process and cyber incident attribution." https://www.dni.gov/files/documents/ICA_2017_01.pdf

Prokop, Andrew. 2019. "All of Robert Mueller's indictments and plea deals in the Russia investigation." *Vox*, March 22, 2019. https://www.vox.com/policy-and-politics/2018/2/20/17031772/mueller-indictments-grand-jury

Smith, David. 2016. "From liberal beacon to a prop for Trump: What has happened to WikiLeaks?" *The Guardian*. October 14, 2016. https://www.theguardian.com/media/2016/oct/14/wiileaks-from-liberal-beacon-to-a-prop-for-trump-what-has-happened

WikiLeaks. 2016. "DNC email database." https://wikileaks.org//dnc-emails/

V

VANDALISM

In general, vandalism is the intentional and unauthorized destruction of property. In the cybercrime context, vandalism is still the intentional and unauthorized destruction of property, but the focus is on intellectual property as opposed to physical property. The United States Bureau of Justice Statistics defines cybervandalism as follows: “the deliberate or malicious damage, defacement, destruction or other alteration of electronic files, data, web pages, or programs” (Rantala, 2008). Under such a definition, the use of computer viruses and other malware that can alter programs on a computer would be considered cybervandalism.

As with acts of vandalism in general, the amount of damage done by cybervandalism can vary. On the less-damaging end of the spectrum, there are incidents in which people will change Wikipedia entries. Wikipedia does permit anyone to change most entries on its site. However, there are times when the changes are arguably malicious. For example, Wikipedia entries have been edited to note that famous people have died, when in fact they have not. Other entries have been edited to dox famous people, adding their personal contact information (Wikipedia, 2019). It appears that those incidents are treated not as criminal matters but rather as a violation of the website’s policies. On the more-damaging end of the spectrum is the hack of Sony Pictures in 2014. Sensitive information was stolen from Sony Pictures in that incident, but it also appears data was erased as part of the hack as well (Siegel, 2014). Accordingly, it would fit the definition of cybervandalism. Indeed, President Barack Obama referred to it as such (Siegel, 2014). It cost Sony Pictures $15 million to clean up the damage done by the hack (Frizell, 2015).

As noted above, cybervandalism generally focuses on damage done to intellectual property, such as computer programs and computer files. However, there can be times where vandalism to physical property can be caused through a cyberattack. Around 2010, it was discovered that Stuxnet—a computer worm—had infiltrated Iran’s Natanz nuclear facility. The worm (suspected by Iran and a number of computer security experts to be deployed by United States and Israeli intelligence officials, such suspicion being based on an Iranian investigation of the incident and the lack of a denial of responsibility from the United States and Israel) allowed the machinery at the nuclear facility to be controlled (Dehghan, 2011). Computers were used to make the centrifuges at the nuclear facility spin rapidly, damaging the centrifuges in the process (Warrick, 2011). In 2016, a water system in the United States was attacked by cybercriminals. They attacked the computers regulating the water supply. Those computers controlled the hardware that regulated the chemical levels in the water supply. With those computers compromised, cybercriminals were able to use the computers to adjust the chemical levels in the water supply. No one suffered illness or other physical harm from this incident (Mahairas and Beshar, 2018).

In addition to actual damage to intellectual property and physical property, cybervandalism can have a psychological impact that is also damaging. In the Iran nuclear facility incident mentioned above, it appears Iran was able to quickly recover from the physical damage done to its equipment. However, knowing that their system was able to be infiltrated did affect confidence of Iranian leaders, making them feel vulnerable (Warrick, 2011). For businesses who are the victims of cybervandalism, consumer confidence can be shaken. Customers may be less likely to shop online at a business whose website was compromised by cybercriminals. This can result in decreased profits for the business that is attacked (Satapathy, 2000).

See also: Doxing; Malware; Operation Olympic Games; Sony Pictures Entertainment Hack; Virus

Further Reading

Dehghan, Saeed Kamali. 2011. "Iran accuses Siemens of helping launch Stuxnet cyber-attack." *The Guardian*, April 17, 2011. https://www.theguardian.com/world/2011/apr/17/iran-siemens-stuxnet-cyber-attack

Frizell, Sam. 2015. "Sony is spending $15 million to deal with the big hack." *Time*, February 4, 2015. http://time.com/3695118/sony-hack-the-interview-costs/

Mahairas, Ari, and Peter J. Beshar. 2018. "A perfect target for cybercriminals." The New York Times, November 19, 2018. https://www.nytimes.com/2018/11/19/opinion/water-security-vulnerability-hacking.html

Rantala, Ramona R. 2008. "Cybercrime against businesses, 2005." Bureau of Justice Statistics. https://www.bjs.gov/content/pub/pdf/cb05.pdf

Satapathy, C. 2000. "Impact of cyber vandalism on the internet." *Economic and Political Weekly* 35, 13: 1059–1061.

Siegel, Robert. 2014. "Was Sony Pictures hack 'cyber vandalism' or something more?" *NPR*, December 22, 2014. https://www.npr.org/2014/12/22/372526841/was-sony-pictures-hack-cyber-vandalism-or-something-more

Warrick, Joby. 2011, February 16. "Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack." *The Washington Post*. http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html

Wikipedia. 2019. "Vandalism on Wikipedia." https://en.m.wikipedia.org/wiki/Vandalism_on_Wikipedia

VICTIMS OF CYBERCRIME

Today, most people do a great deal of their routine activities on the computer. Because of that, there is more opportunity for cybercrime. Becoming a victim of a cybercrime can create long-term harm, which can be emotional, financial, and professional. Emotionally, victims are not able to feel safe if they have been stalked or harassed online. It may hurt someone's ability to look for employment; they may feel unsafe using the internet. Financially, victims can lose thousands of dollars after an attack, or they can be tricked into sending large sums of money to an offender. Professionally, people may have their reputations ruined by false postings of rumors. Victims can be adults, but they can also be children who are groomed to be involved in child pornography. Victims can be men or women, and they can be located anywhere around the globe.

Many victims must spend large amounts of time and money to report a cybercrime. The average case takes 28 days to resolve and costs $334 (Norton, 2010). The victims of cybercrime are a very diverse group. They can be organizations, businesses, governments, or individuals. The effects of a cybercrime can be direct, such as when a particular person or business is directly targeted and feels the full force of an attack; or it can be indirect, which can occur through another person or company. An example of this is when a company is the victim of a cyberattack and an individual's credit card information is stolen. In this case, the victim was not the intended target of the attack, but was indirectly impacted nonetheless.

It is difficult to know how many people become victims of cybercrimes. Many victims choose not to report the cybercrime. Many victims suffer only marginal harm, so they do not take the time to report the crime. Most people also know that the chance that an offender will be caught is slim, so it's not worth reporting. It's often the case that people may not know they have become victims. Also, sometimes, victims are blamed for what happens to them, which makes them even less likely to report an offense. Victims may be embarrassed that they were attacked. Whatever the reason, the crime is not reported to law enforcement.

Victims of cybercrimes often feel angry (58%), annoyed (51%), or even cheated (40%). Three percent of victims believe that it will never happen to them; 80 percent feel that the offenders will not be punished for their crimes (Norton, 2010).

Older people are often victims of cybercrimes, as they often lack technological skills. They are more likely to fall for scams that are sent through e-mail. Older people often do not report if they have been victimized because they are embarrassed or ashamed of what happened. Another vulnerable population is college students. One study on this population found that college students often are not careful when it comes to protecting their online activities because they fail to download the proper security software. Thus, they are more likely to become victims of cybercrime (Choi, 2011).

People who use social media often and who spend time in chat rooms are more likely to be victims of cyberbullying or harassment crimes (Holt et al., 2015). Cyberbullying, if serious enough, may result in the victim's suicide. Victims of cyberstalking tend to be slightly younger, white, male, and have higher reported incomes and education (Nobles et al., 2014).

See also: Cyberbullying; Cyberstalking; Women, Effects on

Further Reading

Choi, Kyung-Shick. 2011. "Cyber-routine activities: Empirical examination of online lifestyle, digital guardians and computer-crime victimization." In *Cyber criminology*, edited by K. Jaishankar. Boca Raton, FL: CRC Press, pp. 229–252.

Help Net Security. 2010. “The emotional impact of cybercrime.” September 8, 2010. https://helpnetsecurity.com/2010/09/08/the-emotional-impact-of-cybercrime/

Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. 2015. *Cybercrime and digital forensics*. London: Routledge.

Jewkes, Yvonne. 2007. “‘Killed by the internet’: Cyber homicides, cyber suicides and cyber sex crimes.” In *Crime online*, edited by Yvonne Jewkes.. Devon, UK: Willan Publishing, pp. 1–11.

Martellozzo, Elena, and Emma A. Jane. 2017. *Cybercrime and its victims*. London: Routledge.

Nobles, Matt R., Bradford W. Reyns, Kathleen Fox, and Bonnie S. Fisher. 2014. “Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample.” *Justice Quarterly* 31, 6: 986–1014.

Norton. 2010. “Cybercrime report: The human impact.” https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf

VIRTUAL PRIVATE NETWORK

A virtual private network (VPN) is a method of connecting to the internet that provides your online activities anonymity. To use a VPN, an encrypted connection is first made between the user’s computer and the server of the VPN provider. The user is then connected to their desired online destination from that server. It is similar to Tor. Tor uses a network of computers—referred to as nodes. A user’s connection is randomly routed through a string of these nodes before connecting the user to their ultimate destination online. Like VPNs, Tor uses encryption while routing a user’s connection (Tor, 2018). This online anonymity can be used both by cybercriminals and users looking to protect themselves from cybercriminals.

For cybercriminals, the appeal of anonymous online activity seems self-evident. A cybercriminal wishing to access online locations that could result in criminal liability—a network they do not have permission to access, a child pornography website, and so forth—they can do so with less risk of being apprehended. For the general-internet user, there are benefits to using a VPN. Cybercriminals can use a sniffer—software that monitors data traveling across a network—to intercept personal information of internet users, such as usernames, passwords, and credit card numbers. If a VPN is used, the information of that user will still be intercepted, but it will be encrypted and thus unreadable by the cybercriminal gathering it. There may be uses of personal information that an internet user may want to protect against that do not involve cybercriminals. In the United States, ISPs are permitted to sell customers’ web browsing history. If a customer uses a VPN, that history will not be visible to the ISP, and thus there will be nothing to sell (Dinha, 2019; Kastrenakes, 2017).

In addition to keeping online activity private from cybercriminals and businesses, a VPN also keeps online activity private from governments. In some countries, the use of VPNs is criminal. In China, operating unauthorized VPNs is subject to punishment. In 2017 and 2018, China prosecuted two separate people for running VPNs (Griffiths, 2018). It would appear China’s concern is that VPNs can be used to circumvent measures put in place by China (known as the Great Firewall of China) to censor certain websites. Russia likewise regulates VPNs, requiring them to register with the government and to block websites banned by the government (Kan, 2019).

According to one study, less than a third of the people surveyed (29%) indicated they used a VPN (Moscaritolo, 2018). While the use of a VPN can increase online security, the use of a VPN does not guarantee that a user will be immune from cybercrime. A VPN does encrypt communications to keep them private from others. However, the VPN provider is still privy to that information. If a VPN provider decides to sell that information (something free VPN providers may are more likely to do as a means of gathering revenue), your information is no longer secure (Dinha, 2019). It is possible that an employee of the VPN provider might access personal information for criminal purposes. In short, a VPN is only as secure as the provider of that VPN. Tor faces similar problems. The operator of the last computer in the random path of computers that a Tor user is processed through (known as the exit node) can observe that user's online activity even though it is not viewable by others. Accordingly, if the operator of an exit node wants to intercept personal information passing through their node and use it for criminal purposes, they can (Franceschi-Bicchierai, 2015).

See also: Privacy; Sniffer; Tor (The Onion Router)

Further Reading

Dinha, Francis. 2019. "The mistakes you're making with your VPN." *Forbes*, March 29, 2019. https://www.forbes.com/sites/forbestechcouncil/2019/03/29/the-mistakes-youre-making-with-your-vpn/#2bb2c07b67cd

Franceschi-Bicchierai, Lorenzo. 2015. "A researcher used a honeypot to identify malicious Tor exit nodes." Motherboard, June 26, 2015. https://motherboard.vice.com/en_us/article/mgbdwv/badonion-honeypot-malicious-tor-exit-nodes

Griffiths, James. 2018. "A software developer just became the latest victim of China's VPN crackdown." CNN, October 10, 2018. https://www.cnn.com/2018/10/10/asia/china-vpn-censorship-intl/index.html

Kan, Michael. 2019. "Russia demands 10 major VPNs censor content or face ban." *PCMag*, March 28, 2019. https://www.pcmag.com/news/367489/russia-demands-10-major-vpns-censor-content-or-face-ban

Kastrenakes, Jacob. 2017. "Congress just cleared the way for internet providers to sell your web browsing history." *CNBC*, March 28, 2017. https://www.cnbc.com/2017/03/28/congress-clears-way-for-isps-to-sell-browsing-history.html

Moscaritolo, Angela. 2018. "Fewer than one-third of consumers use a VPN." *PCMag*, October 5, 2018. https://www.pcmag.com/news/364217/fewer-than-one-third-of-consumers-use-a-vpn

Tor. 2018. "Tor: Overview." https://www.torproject.org/about/overview.html.en

VIRUS

A computer virus is a form of malware. It derives its name from the biological virus—an infectious pathogen that requires a host organism to be able to reproduce.

Computer viruses operate in a similar fashion on computers. A computer virus will infect a host computer and then replicate itself on that host computer. Just as a biological virus can spread, so too can a computer virus spread.

There are several names for various forms of malware, and the distinction between various forms of malware is not universally agreed upon. This applies to viruses. Computer viruses are similar to computer worms. While the exact distinction between viruses and worms is disputed, there are some general differences recognized between the two forms of malware. Viruses—as noted above—as similar to their biological counterparts in that they require a host to replicate. Worms also replicate, but they do not require a host computer to do so. Also, viruses are generally used to describe malware that spreads on a single computer, whereas worms are able to spread over computer networks (Karresand, 2002). This is not to say that viruses cannot spread from one computer to another. However, a virus generally will require some sort of human action (e.g., the owner of the infected computer sending an infected e-mail to someone and that person opening the infected e-mail on their computer) to spread, whereas a worm does not necessarily require a human action. The terms "virus" and "Trojan horse" are often conflated as well. A Trojan horse generally refers to malware that makes its way onto a target computer through some form of deception. How it spreads from there is less specific. Thus, a Trojan horse could be considered a virus by some and a worm by others (Karresand, 2002).

Computer viruses are designed to harm the target computer. What type of harm the virus is designed to cause (i.e., the payload) can vary from virus to virus. The Stuxnet virus, for example, was designed to do physical damage to property. Specifically, it was designed to damage equipment at an Iranian uranium enrichment facility (Weinberger, 2012). The Zeus virus compromises personal information on target computers. The Code Red virus was able to force websites to shut down, including the White House website (Weinberger, 2012). As noted above, there is not a universally agreed-upon distinction between different forms of malware, and it could be argued that these examples are not viruses at all. Nonetheless, these examples do illustrate the point that the harm caused by viruses and other malware is not always well defined. Thus, simply referring to a piece of malware as a virus does not give one a full picture of the threat posed by the malware. It is necessary to describe the features of the malware (e.g., the way the malware spreads, the specific harm it causes) to understand the malware and begin to combat it (Karresand, 2002).

See also: Malware; Operation Olympic Games; Trojan Horse; Worm

Further Reading

Karresand, Martin. 2002. *A proposed taxonomy of software weapons*. Master's thesis in Computer Security at Linköping University, Sweden.

Weinberger, Sharon. 2012. "Top ten most-destructive computer viruses." *Smithsonian*, March 19, 2012. https://www.smithsonianmag.com/science-nature/top-ten-most-destructive-computer-viruses-159542266/

VULNERABILITY

In reference to computers and computer networks, a vulnerability is an aspect of a computer's setup that can be exploited by someone to gain unauthorized access to that computer. Gaining unauthorized access to a computer can be a crime in and of itself in some jurisdictions, such as Minnesota (Minn. Stat. § 609.891) and Texas (Tex. Penal Code § 33.02). Additionally, cybercriminals may gain unauthorized access to a computer to commit further crimes, such as theft or identity theft, among others.

One type of vulnerability a cybercriminal may try to exploit is a software vulnerability. A cybercriminal may be able to assess the software in question and detect a method of bypassing the security measures in place to gain unauthorized access. For example, a computer network might have a hidden bypass programmed into the system, allowing system administrators to access the system with greater ease to perform maintenance and so forth. If a cybercriminal is able to discover this hidden bypass, they can access the system as well. Another example of a software vulnerability is a buffer overflow. In software, a buffer is a temporary data holding area. Buffers will have a set amount of data they can hold. If no preventative code is put in place to check whether the amount of data going into the buffer exceeds the data limit of the buffer, this results in a buffer overflow. An example of a buffer overflow vulnerability can be seen in the case of British Airways's in-flight entertainment system in 2019. That year, Hector Marco—a cybersecurity professor—was on a British Airways flight, and he attempted to test the security system of the entertainment system on the airplane. He input a large amount of text into the system's chat application. This caused the application to crash, exposing the system's vulnerability (Corfield, 2019). In this case, the person discovering the vulnerability was not trying to exploit it. However, cybercriminals can use this method to do just that. If a cybercriminal causes a buffer to overflow by feeding it excessive data, the system can be forced to execute malicious code the cybercriminal has embedded in that data.

Hardware can have vulnerabilities as well. Some hardware vulnerabilities exist due to the use of older hardware. Older hardware may not have the built-in security measures that newer hardware might. Additionally, older hardware is less likely to be supported and maintained by the manufacturer (Lindros, 2016). In some instances, hardware may be physically manipulated to permit unauthorized access to the computer. It is believed this happened with servers manufactured in China for U.S.-based company Super Micro Computer. In an investigation carried out by Amazon prior to acquiring a company that used servers from Super Micro Computer, it was discovered that small microchips were included on the motherboards of the servers that were not included on the original schematic. It is believed the microchips were added by the Chinese military to permit China to monitor the usage of computers within which they were installed (Robertson and Riley, 2018).

Perhaps the most exploitable vulnerability is human vulnerability. Computers and computer networks exist for humans to access and use. For authorized users, access protocols are put in place, such as the creation of a user name and password. Cybercriminals may attempt to deceive authorized users into divulging user names, passwords, and other personally identifying information that may enable them to bypass security measures.

As technology advances and more hardware and software options become available for customers, this in turn provides cybercriminals with new areas to probe for vulnerabilities. Additionally, as computers increase in their mass-computing capabilities, cybercriminals are able to take advantage of that increased ability to more quickly crack the encryption of computer systems (McCullen, 2018). Thus, while technological advances do provide convenience to governments, businesses, and customers, they also provide opportunities to cybercriminals. As we use computer and online technology to assist in the operation of more industries, those industries face potential vulnerability. An example of this would be the water supply in the United States. For some time, water systems were in no way connected to the internet, making infiltration of such systems difficult. As water systems have connected to the internet, their vulnerability has increased. Indeed, in 2016 and 2018, two water systems in the United States were infiltrated. In the 2016 incident, cybercriminals (believed to have ties to Syria) used their unauthorized access to adjust the chemical levels in the water supply (no one suffered illness or was otherwise physically harmed by this incident). In 2018, cybercriminals used their unauthorized access to lock down the computers of a North Carolina water supply in the wake of Hurricane Florence. The hackers demanded a ransom in order for employees to be able to access the system again, but the utility opted to rebuild the system instead (Mahairas and Beshar, 2018).

An issue that businesses, government agencies, and other organizations face with regard to vulnerabilities is vulnerability disclosure. Vulnerability disclosure is where an organization makes the public aware of vulnerabilities in the organization's computer system that it is aware of. There is debate whether an organization should make full and immediate disclosure of vulnerabilities, make no disclosure at all, or do something in between. There are a couple of competing factors at play in this debate. One factor is the impact disclosure will have on future attacks by cybercriminals. The concern is that if an organization discloses the existence of a vulnerability, cybercriminals may attempt to exploit it. The question arises whether an organization should wait until a vulnerability has been fixed before announcing that it existed. One study found that vulnerabilities that were fixed first and then disclosed were attacked by cybercriminals more frequently than vulnerabilities that were not disclosed or vulnerabilities that were disclosed before they were fixed (Arora et al., 2006). Another factor is the impact disclosure has on the speed with which a patch for the vulnerability will be released. One study found that disclosure of a vulnerability does result in a developer releasing a patch more expeditiously (Arora et al., 2010). In the United States, there is no law specifically requiring an organization to make vulnerability disclosures. The Cybersecurity Information Sharing Act of 2015 does permit businesses to share vulnerabilities with government agencies and vice versa. Additionally, it appears that there is a push from the federal government for organizations to have a vulnerability disclosure program in place (Porup, 2018). This is not a program that requires an organization to make vulnerability disclosures. Rather, it is a program that gives security researchers and others that discover vulnerabilities in an organization's system a specific method to report those vulnerabilities to the organization.

See also: Bypass; Hacker and Hacking; Identity Theft; Password; Spyware

Further Reading

Arora, Ashish, Ramayya Krishnan, Rahul Telang, and Yubao Yang. 2010. "An empirical analysis of software vendors' patch release behavior: Impact of vulnerability disclosure." *Information Systems Research*, Vol. 21, No. 1, pp. 115–132.

Arora, Ashish, Anand Nandkumar, and Rahul Telang. 2006. "Does information security attack frequency increase with vulnerability disclosure? An empirical analysis." *Information Systems Frontiers*, Vol. 8, No. 5, pp. 350–362. https://doi.org/10.1007/s10796-006-9012-5

Corfield, Gareth. 2019. "Buffer overflow flaw in British Airways in-flight entertainment systems will affect other airlines, but why try it in the air?" *The Register*, March 8, 2019. https://www.theregister.co.uk/2019/03/08/thales_topseries_vuln/

Lindros, Kim. 2016. "12 hardware and software vulnerabilities you should address now." *Computerworld*, October 12, 2016. https://www.computerworld.com/article/3130119/12-hardware-and-software-vulnerabilities-you-should-address-now.html

Mahairas, Ari, and Peter J. Beshar. 2018. "A perfect target for cybercriminals." *The New York Times*, November 19, 2018. https://www.nytimes.com/2018/11/19/opinion/water-security-vulnerability-hacking.html

McCullen, Robert. 2018. "Cyberthreats: A 10-year perspective." *Forbes*, May 15, 2018. https://www.forbes.com/sites/forbestechcouncil/2018/05/15/cyberthreats-a-10-year-perspective/#29b167525e9e

Porup, J. M. 2018. "Do you need a vulnerability disclosure program? The feds say yes." *CSO*, August 7, 2018. https://www.csoonline.com/article/3294418/do-you-need-a-vulnerability-disclosure-program-the-feds-say-yes.html

Robertson, Jordan and Michael Riley. 2018. "The big hack: How China used a tiny chip to infiltrate U.S. companies." Bloomberg Businessweek, October 4, 2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

W

WAR DIALER

A war dialer is a piece of software that calls a range of phone numbers and notes which of those numbers is connected to a standard telephone, fax machine, or modem (Mienel, 1998; Ryan, 2004). The software is able to determine whether a number is connected to a modem based on the carrier tone produced when that number is called (Berghel, 2004). A log of the numbers associated with a modem—indicating a connection to a computer—is then made.

The term "war dialer" comes from the 1983 movie *WarGames* (Ryan, 2004). In the movie, the protagonist uses the technique described above to locate the computers of a computer game company. The "war" part of the movie's title has been added to the term "dialing" to describe this practice. A war dialer is thus the software that enables one to engage in war dialing.

The legality of war dialing is dubious. The Federal Communications Commission (FCC) regulates the use of autodialers—automatic telephone dialing systems (Federal Communications Commission, 2015). Generally, autodialers that contact people without their consent operate illegally. Though not specifically addressed by name, the definition of autodialers by the FCC would appear to encompass war dialers (Federal Communications Commission, 2015). Thus, if a war dialer were to call a number without the consent of the owner of that number, that act would likely be considered to be in violation of FCC regulations. As will be discussed below, war dialers are generally used as a hacking tool, and thus it is difficult to envision a situation where someone would consent to being called by a war dialer. Thus, the use of war dialers is likely illegal in most (if not all) instances.

Detecting those using war dialers can be more difficult than detecting those who use general autodialers. This is because war dialers have a purpose distinct from general autodialers. General autodialers are generally used by telemarketers and other businesses to contact potential customers. Those who are contacted through an autodialer who do not wish to be contacted will likely know who is contacting them, and they can file a complaint against the offending company accordingly. Someone using a war dialer does not aim to contact anyone. As noted above, a war dialer is simply trying to locate numbers that are connected to a modem. A war dialer can accomplish this without anyone ever answering the phone. If someone picks up the phone—indicating the number that is being called is connected to a telephone and not a modem—the war dialer will simply hang up and move on to the next number (Ryan, 2004). Thus, those who are contacted by war dialer either never answer the phone and are unaware they have been contacted, or they answer the phone to the sound of a disconnected call. In the latter instance, the person contacted will not immediately (if ever) be able to determine who contacted them, making the filing of a complaint difficult, if not impossible.

It is not the inconvenience of receiving a random call from a war dialer that is the primary harm of war dialing. It is what is done with the information obtained from a war dialer that is most harmful. Once a modem-associated phone number is discovered, the owner of the war dialer can then attempt to hack into the computer connected to that modem, or the owner could post that data online for others hackers to make use of (Ryan, 2004). If someone is hacked using data derived from a war dialer, there is a bevy of other crimes that hacker could be charged with, depending on the type of harm that hacker inflicts on the owner of that computer.

It should be noted that war dialers can be used by people other than hackers intending to do harm to the computers they locate. It is possible that a company or government agency may want to hire someone to attempt to hack into their computers to help expose vulnerabilities in their computer system. Indeed, hackers have helped some states test the vulnerability of their electronic voting systems to war dialing and other hacking tactics (Ryan, 2004). In such an instance, the use of a war dialer would likely be legal. The business or agency has consented to the hacker using a war dialer to attempt to access its computers and would thus not appear to run afoul of FCC regulations. Additionally, the hacker has no intent to do harm to the computers if they do gain access. There is a gray area when dealing with benevolent hackers—hackers who hack to alert their targets of the vulnerabilities of their computer network, but do not have the express consent of their targets to engage in such hacking. Those hackers may be in violation of FCC regulations if they do not have consent, but they are likely not in violation of any criminal laws if no harm is caused by their actions (Ryan, 2004).

See also: Cyberwarfare; Wardriving

Further Reading

Badham, John (director), Lawrence Lasker (writer), and Walter F. Parkes (writer). 1983. *WarGames*. Beverly Hills, CA: Metro-Goldwyn-Mayer Studios Inc.

Berghel, Hal. 2004. "Wireless infidelity I: War driving." *Communications of the ACM* 47, 9: 21–26.

Federal Communications Commission. 2015. *Rules and regulations implementing the telephone consumer protection act of 1991; American Association of Healthcare Administrative Management, Petition for Expedited Declaratory Ruling and Exemption; et al*. DA/FCC #: FCC-15-72. Washington, D.C.: Federal Communications Commission.

Meinel, Carolyn P. 1998. "How hackers break in . . . And how they are caught." *Scientific American* 279, 4: 98–105.

Ryan, Patrick S. 2004. "War, peace, or stalemate: Wargames, wardialing, wardriving, and the emerging market for hacker ethics." *Virginia Journal of Law & Technology* 9, 7: 1–57.

WARDRIVING

Wardriving is the process of driving around an area and logging the location and accessibility status of the Wi-Fi networks in that area (Ryan, 2004). Wardriving is similar to war dialing. Wardialing is the process of dialing a range of phone numbers and logging those that are connected to a modem, and thus connected to a computer. As the existence of modem connections via phone line predates Wi-Fi networks, war dialing predates wardriving. Accordingly, the term "wardriving" was derived from "war dialing." The term "war dialing" originally came from the 1983 movie *WarGames*, wherein the movie's protagonist engaged in war dialing (Ryan, 2004). The "war" part of the movie's title was added to the term "dialing" to describe this practice.

Wardriving originated around 1999. The practice was founded by Peter Shipley (Berghel, 2004). The concerns with wardriving are similar to war dialing. With war dialing, once a log of computer-connected phone lines is compiled, hackers can then attempt to gain unauthorized access to those computers through those phone lines. With wardriving, once a log of Wi-Fi networks is compiled, hackers can then attempt to gain unauthorized access to those networks.

With both war dialing and wardriving, those who compile logs will often share those logs on the internet. With wardriving, however, an additional method of disseminating information from those logs has emerged, known as warchalking. Warchalking is the practice of using chalk to make notations of available Wi-Fi networks. These marks can be made on any surface within the range of that Wi-Fi network, such as the wall of a building or the sidewalk. A body of warchalking symbols has emerged—similar to the symbol system used by hobos during the Great Depression—letting warchalkers communicate (Berghel, 2004).

There is a range of harm that can result from wardriving. On one end of the scale, you may simply have people taking advantage of an unsecured Wi-Fi network, gaining internet access without having to pay for it. On the other end, a Wi-Fi network could be accessed with malicious intent, exposing the victim of wardriving to malware attacks, rendering their personal information vulnerable, or similar harms.

Wardriving can also be beneficial. As with war dialing, proactive network administrators may use driving to determine the vulnerabilities in their network (Berghel, 2004). These vulnerabilities can then be addressed, making their network more secure. There is an ethical gray area with wardriving regarding beneficent wardrivers—those who wardrive with the intent to expose Wi-Fi network vulnerabilities, but without the intent to exploit those vulnerabilities. Those wardrivers arguably provide a service to those network owners whose networks have vulnerabilities. However, where the consent of the network owners is not first obtained before looking for these vulnerabilities, there arises a question as to whether such actions are ethical (Ryan, 2004).

See also: Cyberwarfare; Piggybacking; War Dialer

Further Reading

Badham, John (director), Lawrence Lasker (writer), and Walter F. Parkes (writer). 1983. *WarGames*. Beverly Hills, CA: Metro-Goldwyn-Mayer Studios Inc.

Berghel, Hal. 2004. "Wireless infidelity I: War driving." *Communications of the ACM*47, 9: 21–26.

Ryan, Patrick S. 2004. "War, peace, or stalemate: Wargames, wardialing, wardriving, and the emerging market for hacker ethics." *Virginia Journal of Law & Technology* 9, 7: 1–57.

WELCHIA WORM

The Welchia worm (also known as the Nachi worm) was a computer worm, though it is debatable whether the worm would be considered malware. This is because the Welchia worm was apparently designed as a benevolent worm, designed to benefit those to whose computers it spread, not harm them. While the worm was not designed to cause affirmative harm, the worm still accessed computers without the consent of the owner. This unauthorized trespass onto a person's computer could be considered a harm in and of itself, regardless of the ultimate intent of the worm.

The Welchia worm was released on August 18, 2003. It was released in response to the Blaster worm that was released just a week earlier on August 11. The Blaster worm was designed to affect users of Microsoft Windows by causing their computers to continually power on and power off (Gordon, 2003). The Blaster worm apparently had the ultimate goal of shutting down the Microsoft website, but it did not accomplish that goal (Gordon, 2003). Nonetheless, it did infect roughly 16 million computers (Bailey et al., 2005). The Welchia worm was released to combat the Blaster worm. The Welchia worm would infect a computer, delete the Blaster worm, and patch the infected computer to protect against further threat from the Blaster worm (Bransfield, 2003; Naraine, 2003).

Although the Welchia worm was designed eradicate the harm caused by the Blaster worm, it ultimately caused significant harm itself—potentially more harm than it prevented (Bransfield, 2003). The worm bogged down infected networks by forcing computers to attempt to download the patch that would protect against the Blaster worm (Naraine, 2003). Where the Welchia worm came on the heels of the Blaster worm, the problems for those trying to clean up their networks were compounded. In some instances, the worm prevented network administrators from accessing resources necessary to secure their network in wake of the Blaster worm (Naraine, 2003).

The Welchia worm incident does raise some interesting issues. As noted above, it raises an academic question over the definition of malware. Should a program be considered malware only if it intends to do harm, or should it be considered malware if it does in fact cause harm, regardless of intent? Further, if we go with the former definition, how does one ascertain the intent of a piece of software? The Welchia worm incident also raises practical and ethical concerns over the efficacy of designing and releasing benevolent worms. If executed correctly, a benevolent worm could quickly combat and dispatch a harmful worm. However, a worm by definition infiltrates a computer without permission, effectuating a form of cyber-trespass, regardless of the intent of the worm (Bransfield, 2003). Should we aim for efficiency in malware eradication, or should we prioritize the privacy rights of individual computer owners? There is perhaps no easy answer to that question. The Welchia worm, if nothing else, can serve as a cautionary tale of how good intentions can still have catastrophic effects.

See also: Malware; Worm

Further Reading

Bailey, Michael, Evan Cooke, Farnam Jahanian, David Watson, and Jose Nazario. 2005. *The Blaster worm: Then and now*. Washington, D.C.: IEEE Computer Society.

Bransfield, Gene. 2003. *The Welchia worm*. Global Information Assurance Certification Paper, December 18, 2003. North Bethesda, MD: SANS Institute.

Gordon, Jon. 2003. "The Blaster worm explained." *Minnesota Public Radio*, August 29, 2003. http://news.minnesota.publicradio.org/features/2003/08/29_gordonj_virussidebar/ on December 22, 2018.

Naraine, Ryan. 2003. "'Friendly' Welchia worm wreaking havoc." *InternetNews.com*, August 19, 2003. http://www.internetnews.com/ent-news/article.php/3065761/Friendly+Welchia+Worm+Wreaking+Havoc.htm on December 22, 2018.

WHITE-HAT HACKERS

A "white-hat hacker" is someone who breaks into a system with the full knowledge and permission of the officials at a company or organization, a practice often referred to as "penetration testing." The hacker is sometimes an employee of the agency or company, or they may be an outsider who is hired just for the task of testing security programs. These hackers search for security weaknesses or vulnerabilities in the organization's computer systems, allowing those vulnerabilities to be patched before a cybercriminal can discover and exploit them. Some companies will even have contests and award prizes for those employees who are able to discover a weakness in the system. Also called ethical hackers, these individuals are playing a larger role in companies now than ever before. As technology evolves, the hacker's skill set changes as well.

These hackers work within the hacker ethic of "do no harm." Their intent is not to destroy data or harm a computer, unlike a "black-hat hacker," who intends to steal information. If successful over a period of time, these individuals often become security experts. They either establish their own security firms or become consultants for other firms. Their goal is to improve knowledge of computers and increase computer security.

A similar type of hacker is a "gray-hat hacker," who falls in between a white- and black-hat hacker. A gray-hat hacker will carry out both malicious (black-hat) and good (white-hat) hacking, depending on their intent that day, or they may carry out both security and unethical hacking at the same time. The goal of a gray-hat hacker is the same of the white-hat hacker—discovering and exposing a vulnerability—but the gray-hat hacker is willing to break the law to accomplish that goal. A gray-hat hacker may have the intent of embarrassing a company by revealing a weakness in a company's system of which the company is not aware.

Many gray-hat hackers are reformed black hatters—they don't want to hack just for malicious intent. For example, a gray-hat hacker may work independently to get access to a system or network without permission, which would be an illegal act, but then not use that access to destroy or steal data or for harm. Instead, they will inform the organization that they were able to access their system and how they accessed it.

Gray-hat hackers have also been known to help law enforcement. An example of this is the Apple iPhone case in 2016. In December 2015, Syed Rizwan Farook and Tashfeen Malik killed 14 people in San Bernardino, California. The FBI possessed Farook's iPhone but was unable to access the data. Apple refused to break into the phone, so the FBI hired professional hackers to do it. The hackers were paid a fee to find a flaw in the iOS program that could allow them to hack the phone and get any evidence from it. The hackers used a zero-day vulnerability in the software so the FBI could access the data on the phone. Agents believed the phone would reveal information pertaining to the motive or the attack, but they found only information about Farook's work and nothing more about the attack (Tanfani, 2018).

A third type of ethical hacker is a blue-hat hacker. These hackers are "outsiders," or nonemployees, who are hired by a software company to look for vulnerabilities in a program prior to its release. This way, any deficiencies can be found before being put onto the market. The term also refers to the professional hackers who have been hired by Microsoft to expose possible vulnerabilities in their Windows products.

See also: Black-Hat Hackers; Hacker and Hacking; Zero-Day Attacks

Further Reading

Barber, Richard. 2001. "Hackers profiled—Who are they and what are their motivations." *Computer Fraud and Security* 2: 14–17.

Caldwell, Tracey. 2011. "Ethical hackers: Putting on the white hat." *Network Security* 7:10–13.

Kirsch, Cassandra. 2014. "The grey hat hacker: Reconciling cyberspace reality and the law." *Northern Kentucky Law Review* 41: 383–404.

Tanfani, Joseph. 2018. "Race to unlock San Bernardino shooter's iPhone was delayed by poor FBI communication, report finds." *Los Angeles Times*, March 27, 2018. https://www.latimes.com/politics/la-na-pol-fbi-iphone-san-bernardino-20180327-story.html

Zetter, Kim. 2016. "Hacker lexicon: What are white hat, gray hat, and black hat hackers?" *Security*, April 13, 2016. https://www.wired.com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers/

WIKILEAKS

WikiLeaks is an organization that publishes confidential, censored, and other similar material. It serves as a platform through which people can submit confidential records they wish to see made public, while still (to the extent possible) retaining their anonymity.

Julian Assange founded WikiLeaks in 2006. Prior to founding the organization, Assange worked in computer programming. He had also been involved in hacking early on in life. In 1991, he was arrested for hacking into the computer systems of Nortel (Khatchadourian, 2010). He ultimately pleaded guilty to numerous criminal charges related to that incident but avoided incarceration as part of his sentence (Kwek, 2010). As to his motivations for founding WikiLeaks, Assange has said:

> I looked at something that I had seen going on with the world, which is that I thought there were too many unjust acts. And I wanted there to be more just acts, and fewer unjust acts. . . . [Y]ou can change the behavior of many people with a small amount of information. The question then arises as to what kinds of information will produce behavior which is just and disincentivize behavior which is unjust? (Assange, 2014)

Assange saw the censorship of information as detrimental. There are those who might be able to use information to effectuate change of an unjust situation, but if they never receive that information, they will never be able to act on it. Assange noted that many people in possession of sensitive information—such as government employees or employees of large corporations—may self-censor because of fear of the repercussions of sharing that information with the public. For Assange, having an organization like WikiLeaks that would allow individuals to share information with anonymity so they did not have to fear the repercussions of their actions helped negate this self-censorship, which in turn would make important information available that could hopefully be used to curb injustice (Assange, 2014).

Assange described himself at one point as the editor-in-chief of WikiLeaks (*Guardian*, 2010). Due to various legal concerns—some tied to his involvement with WikiLeaks and some not—Assange has been living at the Ecuadoran embassy in London since 2012. This has at times impeded his ability to communicate and be involved with WikiLeaks (Greenfield, 2018). Accordingly, Assange stepped down as editor-in-chief of WikiLeaks in late 2018, handing that position to Kristinn Hrafnsson—an Icelandic journalist who had been a spokesman for WikiLeaks six years preceding her appointment as editor-in-chief (Corfield, 2018).

WikiLeaks has made several noteworthy document leaks, many of them revealing classified government documents. The leak that initially appears to have brought WikiLeaks into the limelight was the 2010 leak of documents by Chelsea Manning—an U.S. Army intelligence officer at the time (Cadwalladr, 2018; Khatchadourian, 2017). The leaks included diplomatic cables, as well as documents concerning the wars in Iraq and Afghanistan. The leak contained footage from U.S. military helicopters in 2010. The footage depicts the slaying of several people in New Baghdad, Iraq; journalists were among those slain (WikiLeaks, 2010). Manning was charged with disclosing these videos and the other documents to WikiLeaks and was ultimately convicted and sentenced to 35 years in prison. President Obama later commuted her sentence, and she is now free (Savage, 2017). Opinions on WikiLeaks and Manning were split following this leak. Manning has been referred to as a traitor by some and as a hero by others (see Valencia, 2010). One study found that the public was nearly split on whether the release of documents related to the war in Afghanistan served or harmed the public interest. Of those who had some knowledge of WikiLeaks disclosures, 42 percent said it served the public interest, and 47 percent said it harmed it. In regards to the disclosure of diplomatic cables, 60 percent of those with some knowledge of the disclosures felt it harmed the public interest, compared to 31 percent who felt it benefited it (Pew Research Center, 2010).

WikiLeaks has disclosed numerous documents since then. In 2011, WikiLeaks released documents related to prisoners held at the detention center at Guantanamo Bay, Cuba. The documents include the names of the detainees, detainee accounts of how they came to be in Guantanamo Bay, assessments of the reliability of the information detainees provided, and a threat assessment of the detainees (WikiLeaks, 2011).

While many of the leaks WikiLeaks publishes are from governments and political groups, it has not limited itself to leaks from those sources. In 2008, WikiLeaks published the secret bibles of Scientology. It has also republished documents initially leaked from other sources. In 2013, it republished communications among climate change researchers allegedly discussing how to manipulate data that does not support their position that climate change was occurring. These e-mails were initially obtained by a hacker and published in November 2009 (Leyden, 2012). As of early 2019, it is still unknown who the hacker was. This incident has come to be known as Climategate.

The response to these disclosures has been mixed. Climate change skeptics claimed the communications were proof that the scientists mentioned in the communications were falsifying evidence of climate change. Others claim the disclosures prove nothing of the sort and that the communications are taken out of context by skeptics wishing to discredit the evidence in support of climate change. The Climategate disclosures do not appear to have had much of an impact on the opinions of climate researchers (see Henig, 2009). WikiLeaks also republished a document archive from Sony in 2015. The documents were initially obtained and disclosed by hackers calling themselves the Guardians of Peace. As there was speculation that the hack was orchestrated by North Korea over its upcoming release of *The Interview*—a comedy whose plot centered on the assassination of North Korean leader Kim Jong-un—WikiLeaks saw the documents to be of public interest. It republished the documents in a form that was more easily searchable (Thielman, 2015).

WikiLeaks found itself in the middle of a document disclosure in 2016 that led some to question the neutrality of WikiLeaks. That year, it released e-mails of presidential candidate Hilary Clinton and other DNC officials (WikiLeaks, 2016). Many of these e-mails were released prior to the 2016 election. Several of the e-mails contained information that appeared to be detrimental to Clinton's presidential run. In one e-mail, it appears Clinton may have been provided a question in advance of a Democratic presidential primary debate by CNN employee Donna Brazile. Also included in the disclosures were statements made by Clinton to Wall Street bankers in a paid speech. In one speech, she said the following about politics: “But if everybody’s watching, you know, all of the back room discussions and the deals, you know, then people get a little nervous, to say the least. So, you need both a public and a private position.” In another e-mail, Clinton’s campaign chairman—John Podesta—criticized Clinton for having terrible instincts. In yet another e-mail, a Clinton spokesman—Josh Schwerin—appeared to indicate that President Barack Obama had lied to the press about his awareness of Clinton’s use of a private e-mail server while serving as President Obama’s Secretary of State (BBC News, 2016). The use of a private e-mail server was an issue over which Clinton came under scrutiny as it potentially violated federal law regarding retention of official communications of government officials.

The content of these leaked communications, coupled with the timing of them before the 2016 presidential election, led to criticisms of WikiLeaks being politically motivated (Smith, 2016). Public opinion of WikiLeaks appeared to change based on one’s political affiliation. In one study, it was found that 12 percent of Republicans who were aware of the e-mail leaks felt the disclosure of the e-mails was harmful to the public, compared to 48 percent of Democrats who were aware of the leaks who felt the disclosure was harmful. This differed from attitudes towards the disclosure of diplomatic cables from Chelsea Manning six years prior. With regard to that disclosure, 75 percent of Republicans who were aware of the leaks found them to be harmful to the public, compared to 53 percent of Democrats who were aware of the leaks finding them to be harmful to the public (Moore, 2016). During the 2008 U.S. presidential election, WikiLeaks disclosed e-mails that had been hacked from Sarah Palin, the Republican vice presidential candidate in that year’s election. Palin criticized WikiLeaks following this incident. Following the disclosure of diplomatic cables from Manning in 2010, Palin said WikiLeaks should be permanently shut down. Following the release of the DNC e-mails, Palin apologized to Assange for her past criticisms (Engel, 2017). Clinton did ultimately lose the 2016 U.S. presidential election. Although the e-mails disclosed by WikiLeaks may have played a part in that, the exact impact of the e-mails on the election is difficult is not impossible to determine (Enten, 2016).

Since the founding of WikiLeaks, several websites have been founded that seek to serve the same purpose. There are several that do exactly what WikiLeaks does, but with a regional focus (e.g., Balkanleaks.eu, Frenchleaks.fr). Some past regional sites (e.g., Thaileaks.info, Tunileaks.appspot.com) were set up to mirror WikiLeaks documents in countries that had blocked WikiLeaks itself (Greenberg, 2011). Other leak sites focus on documents relating to a specific topic. Some past topic-specific leak sites include Unileaks.org (leaks regarding institutions of higher education) and Enviroleaks.org (leaks regarding the state of the environment). There are others that are still in operation as of early 2019, such as Securileaks.org (leaks regarding global security) and Mormonleaks.io (leaks regarding the Mormon church).

See also: Assange, Julian; Hacker and Hacking; Manning, Chelsea; Sony Pictures Entertainment Hack

Further Reading

Assange, Julian. 2014. "Julian Assange: Why I founded WikiLeaks." *Newsweek*, December 24, 2014. https://www.newsweek.com/julian-assange-why-i-founded-wikileaks-294283

BBC News. 2016. "18 revelations from Wikileaks' hacked Clinton emails." October 27, 2016. https://www.bbc.com/news/world-us-canada-37639370

Cadwalladr, Carole. 2018. "I spent seven years fighting to survive': Chelsea Manning on whistleblowing and WikiLeaks." *The Guardian*, October 7, 2018. https://www.theguardian.com/us-news/2018/oct/07/chelsea-manning-wikileaks-whistleblowing-interview-carole-cadwalladr

Corfield, Gareth. 2018. "'Incommunicado' Assange anoints new WikiLeaks editor in chief." *The Register*, September 27, 2018. https://www.theregister.co.uk/2018/09/27/assange_replaced_as_wikileaks_editor/

Engel, Pamela. 2017. "Sarah Palin apologizes to WikiLeaks founder Julian Assange, who she says 'finally opened people's eyes.'" *Business Insider*, January 4, 2017. https://www.businessinsider.com/sarah-palin-apologizes-to-julian-assange-2017-1

Enten, Harry. 2016. "How much did WikiLeaks hurt Hillary Clinton?" *FiveThirtyEight*, December 23, 2016. https://fivethirtyeight.com/features/wikileaks-hillary-clinton/

Greenberg, Andy. 2011. "TooManyLeaks: A list of twenty WikiLeaks copycats." *Forbes*, April 8, 2011. https://www.forbes.com/sites/andygreenberg/2011/04/08/toomanyleaks-a-list-of-twenty-wikileaks-copycats/#2330b43147d9

Greenfield, Patrick. 2018. "Julian Assange to regain internet access at embassy base—Reports." *The Guardian*, October 14, 2018. https://www.theguardian.com/media/2018/oct/14/julian-assange-to-regain-internet-access-in-embassy-base

The Guardian. 2010. "Julian Assange answers your questions." December 3, 2010. https://www.theguardian.com/world/blog/2010/dec/03/julian-assange-wikileaks

Henig, Jess. 2009. "Factcheck: Climategate doesn't refute global warming." *Newsweek*, December 10, 2009. https://www.newsweek.com/factcheck-climategate-doesnt-refute-global-warming-75749

Khatchadourian, Raffi. 2010. "No Secrets: Julian Assange's mission for total transparency." *The New Yorker* 86, 16: 40.

Khatchadourian, Raffi. 2017. "Julian Assange, a man without a country." *The New Yorker*, August 21, 2017. https://www.newyorker.com/magazine/2017/08/21/julian-assange-a-man-without-a-country

Kwek, Glenda. 2010. "Magnet for trouble: How Assange went from simple island life to high-tech public enemy number one." *Sydney Morning Herald*, December 8, 2010. https://www.smh.com.au/technology/magnet-for-trouble-how-assange-went-from-simple-island-life-to-hightech-public-enemy-number-one-20101208-18pb3.html

Leyden, John. 2012. "Climategate cops: We'll NEVER solve email leak hack riddle." *The Register*, July 20, 2012. https://www.theregister.co.uk/2012/07/20/climategate_hack_investigation_killed_off/

Moore, Peter. 2016. "Turnaround in public opinion on latest Wikileaks." *YouGov*, October 25, 2016. https://today.yougov.com/topics/politics/articles-reports/2016/10/25/turnaround-public-opinion-latest-wikileaks

Pew Research Center. 2010. "Most say WikiLeaks release harms public interest." *Pew Research Center*, December 8, 2010. http://www.people-press.org/2010/12/08/most-say-wikileaks-release-harms-public-interest/

Savage, Charlie. 2017. "Chelsea Manning to be released early as Obama commutes sentence." *New York Times*, January 17, 2017. https://www.nytimes.com/2017/01/17/us/politics/obama-commutes-bulk-of-chelsea-mannings-sentence.html

Smith, David. 2016. "From liberal beacon to a prop for Trump: What has happened to WikiLeaks?" *The Guardian*, October 14, 2016. https://www.theguardian.com/media/2016/oct/14/wiileaks-from-liberal-beacon-to-a-prop-for-trump-what-has-happened

Thielman, Sam. 2015. "WikiLeaks republishes all Sony hacking scandal documents." *The Guardian*, April 17, 2015. https://www.theguardian.com/technology/2015/apr/16/wikileaks-documents-sony-hacking-school

Valencia, Nick. 2010. "Berkeley tables resolution to call suspected WikiLeaks soldier 'hero.'" CNN, December 15, 2010. http://www.cnn.com/2010/US/12/15/california.berkeley.wikileaks/index.html

Wikileaks. 2008a. "Church of Scientology's 'Operating Thetan' documents leaked online." https://wikileaks.org/wiki/Church_of_Scientology%27s_%27Operating_Thetan%27_documents_leaked_online

Wikileaks. 2008b. "VP contender Sarah Palin hacked." https://wikileaks.org/wiki/VP_contender_Sarah_Palin_hacked

Wikileaks. 2010. "Collateral murder." https://collateralmurder.wikileaks.org/en/index.html

Wikileaks. 2011. "The Guantanamo files." https://wikileaks.org/gitmo/

Wikileaks. 2013. "CLIMATE: Assortment of statements from East Anglia." https://wikileaks.org/gifiles/docs/40/404797_climate-assortment-of-statements-from-east-anglia-.html

Wikileaks. 2015. "Press release." https://wikileaks.org/sony/press/

Wikileaks. 2016. "DNC email database." https://wikileaks.org//dnc-emails/

Wikileaks. 2018. "Hillary Clinton email archive." https://wikileaks.org/clinton-emails/

WIRETAPPING, *see* PEN REGISTER

WOMEN, EFFECTS ON

As the number of women using the internet and social media increases, more women are reporting becoming victims of cyberviolence. Statistics on this phenomenon are lacking, but initial statistics show that cyberviolence against women is concerning. One study by the UN indicates that 73 percent of women report being abused in some way through an online medium (UN Report, 2015). Another study estimates this number to be 57 percent (Rad Campaign, 2018). Another report by the EU indicates that one in 10 women have been the victim of cyber violence (European Institute for Gender Equality, 2017a). Victimization is also related to age. A study by the Cyber Crime Awareness Foundation found that 73.71 percent of young women between the ages of 18 and 30 reported that they were the victim of cybercrime. This is the highest percentage of cybercrime victimization of all age groups (Mahmud, 2018). Additionally, about 63 percent of women in American report that they know someone who has been the victim of online harassment, whereas only 37 percent of men report this (Women's Media Center, "Research").

Many of the cybercrime offenses that affect women are related to social media. However, it also is a convenient way to harass or bully the women (Halder and

Jaishankar, 2011). Harassment is sometimes carried out through e-mails. An offender may send e-mails that are threatening, offensive, or even bullying in nature. The offender may threaten to cause harm to the victim or their family and friends. Even though many offenders may not go through with the threats, many others choose to carry through with the violence. It has been estimated that users who have female usernames in chatrooms are 25 times more likely to receive messages that are either threatening or sexually explicit than those who use either male names or names that are not identified as either male or female (Women's Media Center, "Research").

Another similar and common cyber offense against women is stalking. About 26 percent of young women admit to being cyberstalked as compared to 7 percent of young men (Women's Media Center, "Research"). There are a multitude of ways an offender can stalk a women online. An offender may follow a woman and then post their daily routine online or what they are wearing, just so the victim knows they are being watched. A stalker may also send multiple e-mails to the offender each day that will bog down the victim's e-mail service. Offenders can even publish a victim's personal information on line, so their home address and phone number will be made available to the public. This is made worse when the offender encourages others to call and leave messages that are embarrassing or hurtful. The offender may hack into a woman's e-mails in order to intercept private communications, which may then be posted online.

Some offenders will create fake e-mails that appear to be coming from a female victim, but they are actually from an offender. This is a form of identity theft. The sent e-mail may include embarrassing or hateful messages, or it may be a plea to send money. Similarly, offenders may imitate a victim in a social media outlet or in a chat room. Those who read the comments will assume they are from the cybercriminals. Other criminals have been known to photoshop a woman's face to a nude body and make it appear that they are involved in obscene behavior. This photo can then be posted online or sent to others through an e-mail. It is often difficult to discern if the photo is real. This technique is referred to as morphing.

A similar offense is to use hate speech or defamation against the victim. Offenders use the computer to publish untrue or false comments about a person. Some offenders will make critical comments about a woman, her body, a criminal background, or her private sexual history. They may make threats to release information if the victim doesn't do something, such as send money.

Women also are likely to become victims of cyber theft, particularly the e-mails that promise to provide money for helping another person. Since women tend to be the ones who care for others, they are more likely to fall victim to a plea for help, even if it is not real.

Human Trafficking and Sex Trade

A dangerous issue that affects women is sex-oriented crimes. One of those is human trafficking and the sex trade. Female victims are solicited through online sites, and after a series of e-mails geared toward making the victim comfortable with the offender, they may meet in person and be lured into committing sex offenses. Women are sometimes forced to "sex chat" with offenders, who then post those messages online for other to see.

There are also thousands of sites dedicated to pornography and online prostitution, and the number of those sites is increasing regularly. One study estimated that there were 300,000 internet websites devoted to pornography, which was a 350 percent increase from the previous year (Hughes, 2003). Another study estimated that 37 percent of the internet is made up of pornographic matter (Ward, 2013).

Women are frequently the victims of "revenge porn" whereby an offender will post sexually graphic images of them without their permission or consent. The photos or videos may have been captured during a previous relationship, or the offender may have hacked into the personal files of the woman. Females comprise upwards of 95 percent of the victims of this kind of attack (Women's Media Center, "Online")

Many sites include opportunities for escort services that tend to be more high-end or upscale, and are usually charge people by the hour. Here, the women involved tend to be more attractive (Sharp and Earle, 2002, p. 37). There are also prostitution sites made up of "independent" workers, who are women who have chosen not to work for another person. The prices charged are less than for female escorts. The websites for these women tend to be less professional and include more pornographic pictures. Another type of online prostitution is massage parlors. For these, the prices tend to be cheaper but do not include the price for any sexual acts (Sharpe and Earle, 2002).

Many women become the victims of romance schemes. It is estimated that 63 percent of victims in romance scams are female, with an average age of 50. Moreover, it is estimated that women involved in these scams lose twice as much money than men (Peachey, 2019). The women often meet someone on an online dating site and fall in love. The offender asks for money so they can pay off debts or so they can travel to see the woman. Unfortunately, once the money is received, the person is never heard from again.

The women who become victims of cybercrimes often suffer both short- and long-term consequences. In the short term, the victims will lose money and feel scared or threatened. In the long term, female victims may find their reputations harmed or even ruined. Their relationships with others can also be harmed or ruined if posted comments are embarrassing or harmful. In some cases, the harassment can lead to the loss of a job or career opportunities. The crimes can also lead to emotional effects, including suicide or other violent acts (European Institute for Gender Equality, 2017b; Judge, 2019).

See also: Cyberbullying; Cyberstalking

Further Reading

European Institute for Gender Equality. 2017a. "Cyber violence against women and girls." https://en.unesco.org/sites/default/files/genderreport2015final.pdf

European Institute for Gender Equality. 2017b. “Cyber violence is a growing threat, especially for women and girls.” June 19, 2017. https://eige.europa.eu/news/cyber-violence-growing-threat-especially-women-and-girls

Halder, Debarati, and K. Jaishankar. 2011. “Online social networking and women victims.” In *Cyber criminology*, edited by K. Jaishankar. Boca Raton, FL: CRC Press, pp. 299–316.

Hughes, Donna. 2003. Prostitution Online. *Journal of Trauma Practice* 2: 3–4.

Judge, Kristen. 2019. “How to support cybercrime victims.” *PoliceOne*, April 25, 2019. https://www.policeone.com/investigations/articles/483667006-How-to-support-cybercrime-victims/

Mahmud, Faisal. 2018. “Cyber-crime and the vulnerability of the fairer gender.” *Fintech*, July 3, 2018. http://www.fintechbd.com/cyber-crime-and-the-vulnerability-of-the-fairer-gender/

Peachey, Kevin. 2019. “Women ‘victims in 63% of romance scams.’” *BBC News*, February 10, 2019. www.bbc.com/news/business-47176539

Rad Campaign. 2018. “Online harassment: Still a big problem and getting worse.” http://onlineharassmentdata.org/

Sharp, Keith, and Sarah Earle. 2002. “Cyberpunters and cyberwhores: Prostitution on the internet.” In *Dot.cons: Crime, deviance and identity on the internet*, edited by Yvonne Jewkes. Devon, UK: Willan Publishing, pp. 36–52.

U.N. Broadband Commission for Digital Development Working Group on Broadband and Gender. 2015. “Cyberviolence against women and girls: A world wide wake-up call.” www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf

Ward, Mark. 2013. “Web porn: Just how much is there?” *BBC News*, July 1, 2013. https://www.bbc.com/news/technology-23030090

Women’s Media Center. n.d. “Online abuse 101.” http://www.womensmediacenter.com/speech-project/online-abuse-101#faq

Women’s Media Center. n.d. “Research & statistics.” https://www.womensmediacenter.com/speech-project/research-statistics

WORM

Generally speaking, a computer worm is a form of malware. It is a program that gains unauthorized access to a computer and, in most instances, causes harm to that computer. In this regard, it is similar to a computer virus. How it differs from a computer virus, however, has not been definitively established. There are various definitions of both worms and viruses (Karresand, 2002). Among these definitions, there are some common aspects that distinguish worms from viruses. First, unlike a computer virus, a computer worm is self-replicating. In other words, where a computer virus requires some sort of initial action by a human to spread and infect a computer, a computer worm is designed to spread and infect computers on its own. Second, worms tend to spread over computer networks while viruses tend to spread just on the infected computer (Karresand, 2002).

A computer worm can be designed to carry out a variety of difference malicious tasks on an infected computer. The worm could download spyware or ransomware to the infected computer, steal personal information, or allow the sender of the worm to remotely access an infected computer. One type of attack that is somewhat unique to computer worms is the ability to overload the processing ability of a computer, causing it to shut down. A computer worm is able to do this because it is self-replicating. It is able to make numerous copies of itself on an infected computer, to the point where the infected computer is not able to match the processing power necessary to run all copies of that worm. This is not to say a computer virus could not accomplish the same thing, albeit with some human-initiated action. However, the nature of computer worms makes such an attack easier to carry out with a computer worm.

As noted above, a worm is not limited to replicating itself on the originally infected computer or other electronic device. Worms can spread to other electronic devices without human intervention as well. To spread from one electronic device to another, those electronic devices would have to be connected in some fashion—the internet being perhaps the most likely way. The worm could use some sort of messaging system—such as e-mail or an instant messaging application—to help itself spread.

The damage done by computer worms can be extensive. The Code Red worm is one of the most damaging computer worms to date. The worm infected just under a million systems overall, a quarter of those within the first nine hours of operation. The damage resulting from the work was in excess of $2 billion (Rhodes, 2001). As mentioned above, the damage can extend beyond economic damage (e.g., private data can be compromised).

Not all computer worms are released with the intent to do harm. There are worms that have benevolent purposes. Some worms (e.g., Welchia, CodeGreen) were released specifically to counteract malicious worms. Although these worms are released with benevolent intent, there are still ethical concerns regarding these types of worms because, even though they are released with the intent to do good, the worms still access computers without the consent of the owner. Also, even though the purpose of these worms is to help the owners of the accessed computers, there can be unintended consequences of the worms that end up doing harm (Bransfield, 2003).

See also: Code Red; Malware; Melissa Worm; Nimda; Payload; Virus; Welchia Worm

Further Reading

Bransfield, Gene. 2003. *The Welchia worm*. Global Information Assurance Certification Paper, December 18, 2003. North Bethesda, MD: SANS Institute.

Karresand, Martin. 2002. A proposed taxonomy of software weapons. Master's thesis in Computer Security at Linköping University, Sweden.

Rhodes, Keith A. 2001. *Testimony before the Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform, House of Representatives*. Washington, D.C.: United States General Accounting Office.

Y

YOUTH AND CYBERCRIME

Like many people, young people rely on the internet for everyday activities, from communicating with friends to shopping, schoolwork, and video games. Most youth today grew up with technology and devices, utilizing the internet daily, and have become comfortable with it. At the same time, they are more likely to give out personal information, especially on social media. They are also likely to have passwords that are easy to hack. As they use the internet more, young people are becoming victims of cybercrimes. Also, because young people tend to use technology more often, they are more likely to become victims of online crimes when compared to adults.

As victims of cybercrimes, youth are harassed by peers, are exposed to pornography, and are victims of identity theft. The exact number of young victims of cybercrime is difficult to know for sure, as they are not always reported to law enforcement. One survey found that 5.3 percent of youth aged 15–24 years were reported that they were victims of cybercrime in 2008 (Oksanen and Keipi, 2013). They are likely to be victims of cyberbullying, pirating materials, and sexting, but they are also offenders of cybercrimes.

Cyberbullying is a growing problem among young people and in schools. This is the use of technology, and especially social media, to threaten, harass, or embarrass others. It is often linked to low self-control that is often found in young people. It has also been linked to peer pressure—many children who participate in online bullying are influenced by their friends to do so. According to the National Crime Prevention Council, 17 percent of youth reported that someone had been posting untruths about them online, and 13 percent learned that an offender was pretending to be them and posting information to others; 10 percent of youth were reportedly victimized when someone unknown to them posted unflattering pictures of them online, without their permission (National Crime Prevention Council, n.d.).

Youth are likely to pirate music and movies, simply because young people often do not have a lot of extra money. One study on pirating activities by youth found that 52 percent of eighth graders had pirated either a movie, music, or games in their lifetime; 44 percent reported that they pirated in the past year, and 35.1 percent admitted that they pirated sometime in the previous month. When it came to pirating most often, 16.1 percent pirated on a daily basis. When 11th grade students were questioned about their pirating behavior, those number increased significantly. When it came to older students, 72.3 percent admitted to pirating behavior at some point in their lifetime. Moreover, 63.8 percent of eleventh graders agreed that they pirated something in the previous year, with 52.8 percent reporting something in the past month and 25 percent carrying out pirating behavior on a daily basis (Gunter et al., 2010). In another study, it was found that males were more likely to show attitudes that were more favorable toward music piracy than females (Malin and Fowers, 2009).

Sexting is another offense that is common among young people. They are likely to send and/or receive sexually explicit or graphic images through their phones. The images can be saved or forwarded to others. In some states, youth who do this can be charged with possession of child pornography. Any youth convicted of sexting and transmitting pornography may be labelled as a sex offender. A study on sexting found that about 13 percent of youth in the study had sent either a nude or partially nude photo of themselves to another person through a text within the previous year (Ricketts et al., 2015).

Conversely, youth are frequently the offenders when it comes to cybercrimes. They often have the technical skills needed to carry out cybercrimes. Youth see cybercrime as an opportunity to make quick money. The number of youth prosecuted for crimes under the Unauthorized Computer Access Law has increased fourfold between 2003 and 2013 (Kar, 2013). Research found that peers who have friends who engage in cybercrime are more likely to commit cybercrimes themselves. Often those involved are kids with low self-control (Holt et al., 2012).

To protect youth from becoming victims of cybercrimes, law enforcement and other experts recommend that parents remain involved in the children's online behavior. They should watch the child's activities on social media and the internet. Parents should, even at an early age, teach children to be more aware of the importance of online security and the use of better passwords. They should also stress the need to caution and restraint when posting personal information online.

See also: Cyberbullying; Sexting

Further Reading

Gunter, Whitney D., George E. Higgins, and Roberta E. Gealt. 2010. "Pirating youth: Examining the correlates of digital music piracy among adolescents." *International Journal of Cyber Criminology* 4, 1–2: 657–671.

Holt, Thomas, Adam M. Bossler, and David C. May. 2012. "Low self control, deviant peer associations, and juvenile cybercrime." *American Journal of Criminal Justice* 37, 3: 378–395.

Kar, Saroj. 2013. "Youth cyber crimes on the rise, but how ready are we?" *SiliconAngle*, September 24, 2013. https://siliconangle.com/2013/09/24/youth-cyber-crimes-onthe-rise-but-how-ready-are-we/

Malin, J., and B. J. Fowers. 2009. "Adolescent self-control and music and movie piracy." *Computers in Human Behavior*, 25, 718–722.

Marcum, Catherine D. 2011. "Adolescent online victimization and constructs of routine activities theory." In *Cyber criminology*, edited by K. Jaishankar. Boca Raton, FL: CRC Press, pp. 253–276.

Nasi, Mati, Atte Oksanen, Teo Keipi, and Pekka Rasanen. 2013. "Cybercrime victimization among young people: A multi-nation study." *Journal of Scandinavian Studies in Criminology and Crime Prevention* 16, 2: 203–210.

National Crime Prevention Council. n.d. "Cyberbullying." http://www.ojp.gov/cds/internetsafety/NCPC/ Stop%20Cyberbullying%20Before%20It%20Starts.pdf

Oksanen, A., and T. Keipi. 2013. "Young people as victims of crime on the internet: A population based study in Finland." *Vulnerable Children and Youth Studies*, 8, 298–309.

Ricketts, Melissa, Carrie Maloney, Catherine Marcum, and George Higgins. 2015. "The effect of internet related problems on the sexting behaviors of juveniles." *American Journal of Criminal Justice* 40, 2: 270–284.

Z

ZERO-DAY ATTACKS

A zero-day attack is a when a cybercriminal exploits or takes advantage of an unknown security vulnerability (a weakness or flaw) in a computer program to compromise the integrity or confidentiality of the product. Once a hacker is able to find a glitch in a software program (the vulnerability), they can install malware such as viruses or worms into a network. The criminal can edit the program and make it do something other than it is intended. It is called a zero-day attack (or a zero-day vulnerability) because there are zero days to fix the problem as the vulnerability will be discovered after the attack has occurred. Day zero is the day when the owner learns of the vulnerability.

Most of the time, the creator of software is not aware of a vulnerability, so no fix (called a patch) has been created. The hacker who discovers the vulnerability will be able to control that computer until the attack is discovered. Cybercriminals like these types of attacks because every user of the software is then vulnerable. Anyone who downloads that software program may also have the malware uploaded into their system. Zero-day attacks are often difficult to find, so the hacker has a long time to gather information from those affected. Moreover, as there could be a long time between when the malware is uploaded and when it is found, there is a long time during which the infected malware can spread.

In some cases, the cybercriminal will discover a vulnerability and sell the information on the dark web for others to use. They will sell zero-day vulnerabilities on a zero-day market. There are three types of zero-day markets. One is the black market or the dark web. Here, hackers will sell the details about the vulnerability to other cybercriminals, who can use the attack to upload malware to steal passwords and credit card information. Because vulnerabilities are difficult to find, they are in high demand and also very expensive on the dark web. They will often cost between a few thousand dollars to $300,000, depending on the extent of the vulnerability. As the majority of vulnerabilities can only be used once, they are more expensive (Ablon et al., 2014).

The second market is the white market, which comprises researchers and hackers who will find a vulnerability and then contact the software vendor or owners and give that information to them so the weakness can be fixed. The hacker may ask for money and demand payment before they provide the information. Businesses will often buy information about a vulnerability so they can find a patch before it is discovered by a hacker. The third market is the gray market, where researchers and hackers will sell the information about zero-day exploits to military or intelligence agencies to use for intelligence reasons.

A zero-day attack will always be successful. The software creator does not know about the weakness, so they are not aware that the program could be hacked. Moreover, because the vulnerability is unknown, there is no patch or fix available. By the time the attack is discovered, it has probably already allowed the attacker to gather personal information from victims. These attacks can cause a lot of damage because they can be attacking a system for a long time before the owner is aware of it.

If a vulnerability becomes known to a hacker, they will often keep it a secret until they have a chance to either use it or sell it to another hacker. If it is discovered by a company, officials will typically work to fix it as quickly as they can. Some officials may choose to announce the problem to the public and encourage users to patch it before too much harm occurs.

A similar term is "zero-day virus" or "zero-day malware," which is a previously unknown virus or malware. These are particularly damaging because there will be no antivirus software or patch to remove the virus from a computer.

The Stuxnet virus was a zero-day attack carried out by the United States against Iran. It began in 2006 when the United States sought to access the computer systems of a nuclear power plant in that country. They were able to upload malware into the computer system of the plant that disabled almost 1,000 centrifuges in the plant. Officials in the plant said they discovered the bug and contained it. The 2014 cyberattack on Sony was also a zero-day attack. Here, the hackers uploaded malware to the Sony system to get access to it and then gained access to confidential documents.

It is difficult to defend against a zero-day attack because the weakness is unknown. However, there are steps that can be taken to mitigate damage from a zero-day attack. The most important is to install security software and keep it updated. That way, if malware is uploaded, it may be discovered before much data is stolen. Another step is to keep up to date with any patches the company makes available.

A half-day attack, also called a one-day or two-day attack, occurs when the creator of the software is aware of the vulnerability and has made a patch available to users, and even though the consumers are aware of the patch, they have not applied it yet. This delay in applying the fix gives the cybercriminal time to steal data from the victim.

See also: Dark Web; Malware; Operation Olympic Games

Further Reading

Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay. 2014. *Markets for cybercrime tools and stolen data*. Washington, D.C.: Rand Corporation.

Morgenstern, Joe. 2016. "Zero Days." *Wall Street Journal*, July 8, 2016. https://www.wsj.com/articles/zero-days-review-the-new-front-lines-1467918680

Zetter, Kim. 2014. *The countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. New York: Crown Publishers.

Bibliography

Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay. 2014. *Markets for Cybercrime Tools and Stolen Data*. Washington, D.C.: Rand Corporation.

Akdeniz, Yaman. 2008. *Internet Child Pornography and the Law: National and International Responses*. Burlington, VT: Ashgate Publishing.

Akhgar, Babak, Andrew Staniforth, and Francesca Bosco. 2014. *Cybercrime and Cyber-Terrorism Investigator's Handbook*. Waltham, MA: Elsevier.

Ansari, Sabeel, S. G. Rajeev, and H. S. Chandrashekar. 2003. "Packet Sniffing: A Brief Introduction." *IEEE Potentials*, Vol. 21, No. 5, pp. 17–19.

Arora, Ashish, Ramayya Krishnan, Rahul Telang, and Yubao Yang. 2010. "An Empirical Analysis of Software Vendors' Patch Release Behavior: Impact of Vulnerability Disclosure." *Information Systems Research*, Vol. 21, No. 1, pp. 115–132.

Arora, Ashish, Anand Nandkumar, and Rahul Telang. 2006. "Does Information Security Attack Frequency Increase with Vulnerability Disclosure? An Empirical Analysis." *Information Systems Frontiers*, Vol. 8, No. 5, pp. 350–362. doi:10.1007/s10796-006-9012-5

Balganesh, Shyamkrishna. 2013. "Copyright Infringement Markets." *Columbia Law Review*, Vol. 113, No. 8, pp. 2277–2332.

Banks, James. 2010. "Regulating Hate Speech Online." *International Review of Law, Computers and Technology*, Vol. 24, No. 3, 233–239.

Bauman, Sheri. 2011. *Cyberbullying: What Counselors Need to Know*. Alexandria, VA: American Counseling Association.

Berghel, Hal. 2004. "Wireless Infidelity I: War Driving." *Communications of the ACM*, Vol. 47, No. 9, pp. 21–26.

Bidgoli, Hossein. 2006. *Handbook of Information Security*. New York: John Wiley and Sons.

Binder, Nellie Veronika. 2018. "From the Message Board to the Front Door: Addressing the Offline Consequences of Race- and Gender-Based Doxxing and Swatting." *Suffolk University Law Review*, Vol. 55, pp. 55–75.

Blanchette, Jean Francois. 2012. *Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents*. Cambridge, MA: MIT Press.

Blane, John V. 2003. *Cybercrime and Cyberterrorism: Current Issues*. New York: Novinka Books.

Bocij, Paul. 2004. *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*. Westport, CT: Praeger.

Bocij, Paul. 2006. *The Dark Side of the Internet: Protecting Yourself and Your Family from Online Criminals*. Westport, CT: Praeger.

Bose, Indranil, and Alvin Chung Man Leung. 2014. "Do phishing alerts impact global corporations? A firm value analysis." *Decision Support Systems*, Vol. 64, pp. 67–78.

Boyd, Danah M., and Nicole B. Ellison. 2007. "Social Network Sites: Definition, History, and Scholarship." *Journal of Computer-Mediated Communication*, Vol. 13, No. 1, pp. 210–230.

Boyle, Randall J. 2013. *Corporate Computer Security*. Boston, MA: Pearson.

Brenner, S. W. 2008. *Cyberthreats: The Emerging Fault Lines of the Nation State.* New York: Oxford University Press.

Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab, Brigitte Bouhours, and Steve Chon. 2014. "Organizations and Cyber Crime: An Analysis of the Nature of Groups engaged in Cyber Crime." *International Journal of Cyber Criminology*, Vol. 8, No. 1, pp. 1–20.

Brody, Richard G., Elizabeth Mulig, and Valerie Kimball. 2007. "Phishing, Pharming and Identity Theft." *Academy of Accounting and Financial Studies Journal*, Vol. 11, No. 3, pp. 43–56.

Bryant, Robin, and Sarah Bryant. 2014. *Policing Digital Crime*. Farnham, Surrey: Ashgate.

Calce, M., and C. Silverman. 2008. *Mafiaboy: How I Cracked the Internet and Why It's Still Broken*. Toronto: Penguin Group Canada.

Caravut, Sinchai. 2008. *Multiple Logs Analysis for Detecting Zero-Day Backdoor Trojans*. Cleveland, OH: Cleveland State University Press.

Carr, Jeffrey. 2010 *Inside Cyberwarfare*. Sebastopol, CA: O'Reilly Media.

Casey, Eoghan. 2004. *Digital Evidence and Computer Crime*. Boston, MA: Elsevier.

Clough, Jonathan. 2015. *Principles of Cybercrime*. Cambridge, UK: Cambridge University Press.

Cohn, William A. 2007. "Yahoo's China Defense." *New Presence: The Prague Journal of Central European Affairs*, Vol. 9, No. 3, pp. 30–33.

Coleman, Gabriella. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London: Verso.

Commission on the Theft of American Intellectual Property. 2017. *Update to the IP Commission Report*. Seattle, WA: The National Bureau of Asian Research.

Council of Europe. 2007. *Cyberterrorism: The Use of the Internet for Terrorist Purposes*. Strasbourg Cedex, France: Council of Europe Publishing.

Denning, Peter J. 1989. *The ARPANET after Twenty Years*. Moffett Field, CA: Research Institute for Advanced Computer Science.

Elisan, Christopher C. 2015. *Advanced Malware Analysis.* New York: McGraw-Hill.

Englander, Elizabeth Kandel. 2013. *Bullying and Cyberbullying: What Every Educator Needs to Know*. Cambridge, MA: Harvard Education Press.

Essany, Michael. 2012. *LulzSec: How a Handful Of Hackers Brought the US Government to Its Knees: 50 days of Lulz*. New York: Hyperlink.

Furnell, Steven. 2002. *Cybercrime.* Boston, MA: Addison-Wesley.

Gillespie, Alisdair A. 2016. *Cybercrime: Issues and Debates*. New York: Routledge.

Goel, Sanjay, and Hany A. Shawky. 2009. "Estimating the Market Impact of Security Breach Announcements on Firm Values." *Information & Management*, Vol. 46, pp. 404–410.

Hafner, Katie, and John Markoff. 1991. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon & Schuster.

Harrell, Erika. 2015 (revised 2017). *Victims of Identity Theft, 2014*. Washington, D.C.: Bureau of Justice Statistics.

Hileman, Garrick, and Michel Rauchs. 2017. *Global Cryptocurrency Benchmarking Study*. Cambridge, UK: Cambridge Centre for Alternative Finance.

Hill, Joshua B. and Nancy E. Marion. 2016. *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century.* Santa Barbara, CA: ABC-CLIO.

Holt, Thomas J. 2017. *Cybercrime through an Interdisciplinary Lens*. New York: Routledge.

Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. 2018. *Cybercrime and Digital Forensics*. New York: Routledge.

Holt, Thomas J., George W. Burruss, and Adam M. Bossler. 2015. *Policing Cybercrime and Cyberterror*. Durham, NC: Carolina Academic Press.

Howard, Philip N., Aiden Duffy, Deen Freelon, Muzammil Hussain, Will Mari, and Marwa Mazaid. 2011. "Opening Closed Regimes: What Was the Role of Social Media during the Arab Spring?" Seattle: University of Washington.

Jaishankar, K. 2011. *Cyber Criminology.* Boca Raton, FL: CRC Press.

Jewkes, Yvonna. 2007. *Crime Online*. Devon, UK: Willan Publishing.

Jordan, T., and P. Taylor. 2004. *Hacktivism and Cyber Wars*. London: Routledge.

Jung, Jeyong, and Julak Lee. 2017. "Contemporary Financial Crime." *Journal of Public Administration and Governance*, Vol. 7, No. 2, pp. 88–97.

Karresand, Martin. 2002. *A Proposed Taxonomy of Software Weapons.* Master's thesis in Computer Security at Linköping University, Sweden.

Kehoe, Brendan P. 1996. *Zen and the Art of the Internet: A Beginner's Guide.* Upper Saddle River, NJ: Prentice Hall.

Knotts, Rose, and Tom Richards. 1989. "Computer Security: Who's Minding the Store?" *The Academy of Management Executive*, Vol. 3, No. 1, pp. 63–66.

Kremling, Janine, and Amanda M. Sharp Parker. 2018. *Cyberspace, Cybersecurity, and Cybercrime*. Thousand Oaks, CA: Sage.

Kshetri, Nir. 2010. "Diffusion and Effects of Cyber-Crime in Developing Economies." *Third World Quarterly*, Vol. 31, No. 7, pp. 1057–1079.

Lapsley, Phil. 2013. *Exploding the Phone*. New York: Grove Press.

Law Library of Congress. 2018. *Regulation of Cryptocurrency around the World*. Washington, D.C.: The Law Library of Congress.

Lemley, Mark A., and R. Anthony Reese. 2004. "Reducing Digital Copyright Infringement without Restricting Innovation." *Stanford Law Review*, Vol. 56, No. 6, pp. 1345–1434.

Leukfeldt, E. Rutger, Anita Lavorgna, and Edward R. Kleemans. 2016. "Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime." *European Journal on Criminal Policy and Research*. doi:10.1007/s10610-016-9332-z

Levine, Yasha. 2018. *Surveillance Valley: The Secret Military History of the Internet*. New York: Public Affairs.

Li, Xingan. 2017. "A Review of Motivations of Illegal Cyber Activities." *Criminology & Social Integration Journal*, Vol. 25, No. 1, pp. 110–126.

Littman, Jonathan. 1997. *The Watchman: The twisted Life and Crimes of Serial Hacker Kevin Poulsen*. Boston, MA: Little, Brown and Company.

Long, Johnny. 2008. *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. Rockland, MA: Syngress.

Martellozzo, Elena, and Emma A. Jane. 2017. *Cybercrime and Its Victims*. London: Routledge.

Martin, Keith M. 2017. *Everyday Cryptography: Fundamental Principles and Applications*. Oxford: Oxford University Press.

McDonald, Aleecia M., and Lorrie Faith Cranor. 2008. "The Cost of Reading Privacy Policies." *I/S: A Journal of Law and Policy for the Information Society*, Vol. 4, No. 3, pp. 543–568.

McQuade, S. C. 2006. *Understanding and Managing Cybercrime*. Boston, MA: Pearson/Allyn and Bacon.

McWilliams, Brian. 2004. *Spam Kings: The Real Story Behind the High-Rolling Hucksters Pushing Porn, Pills and @*#?% Enlargements*. Cambridge, UK: O'Reilly.

Middleton, Bruce. 2001. *A History of Cyber Security Attacks: 1980 to Present*. Boca Raton, FL: CRC Press.

Mirkovic, Jelena, Sven Dietrich, David Dittrich, and Peter Reiher. 2005. *Internet Denial of Service: Attack and Defense Mechanisms*. Upper Saddle River, NJ: Prentice-Hall.

Mitnick, K. D., and W. L. Simon. 2002. *The Art of Deception: Controlling the Human Element of Security.* New York: Wiley Publishing.

Mitnick, K. D., and W. L. Simon. 2005. *The Art of Intrusion*. Indianapolis, IN: Wiley.

Moore, Daniel, and Thomas Rid. 2016. "Cryptopolitik and the Darknet." *Survival*, Vol. 58, pp. 7–38.

Mouton, Francois, Louise Leenan, and H. S. Venter. 2016. "Social engineering Attack Examples, Templates and Scenarios." *Computers and Security*, Vol. 59, pp. 186–209.

Mueller, Robert S. 2019. "Report on the Investigation into Russian Interference in the 2016 Presidential Election." Volume 1. United States Department of Justice. https://www.justice.gov/storage/report.pdf

Mullen, P. E., M. Pathe, and R. Purcell. 2009. *Stalkers and Their Victims.* New York: Cambridge University Press.

Musa, Sarhan M. 2018. *Network Security and Cryptography: A Self-Teaching Introduction*. Dulles, VA: Mercury Learning and Information.

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." https://bitcoin.org/bitcoin.pdf

Office of the Director of National Intelligence. 2017. *Assessing Russian Activities and Intentions in Recent U.S. Elections*. Washington, D.C.: Office of the Director of National Intelligence.

Office of the Inspector General. 2018. *A Special Inquiry Regarding the Accuracy of FBI Statements Concerning Its Capabilities to Exploit an iPhone Seized during the San Bernardino Terror Attack Investigation*. Washington, D.C.: Office of the Inspector General.

Olson, Parmy. 2012. *We Are Anonymous*. New York: Little, Brown and Company.

Pallante, Maria A. 2013. "The Next Great Copyright Act." *The Columbia Journal of Law & the Arts*, Vol. 36, No. 3: 315–344.

Phillips, Whitney. 2015. *This Is Why We Can't Have Nice Things: Mapping the Relationship between Online Trolling and Mainstream Culture*. Cambridge, MA: MIT Press.

Pickett, K. H. Spencer, and Jennifer M. Pickett. 2002. *Financial Crime Investigation and Control*. New York: John Wiley & Sons, Inc.

Pirounias, Sotirios, Dimitrios Mermigas, and Constantinos Patsakis. 2014. "The Relation between Information Security Events and Firm Market Value, Empirical Evidence on Recent Disclosures: An Extension of the GLZ Study." *Journal of Information Security and Applications*, Vol. 19, pp. 257–271.

Poller, Andreas, Ulrich Waldmann, Sven Vowe, and Sven Turpe. 2012. "Electronic Identity Cards for User Authentication—Promise and Practice." *IEEE Security & Privacy*, Vol. 10, No. 1, pp. 46–54.

Pontell, Henry N., Gilbert Geis, and Gregory C. Brown. 2011. "Internet Gambling." In *Cyber Criminology*, edited by J. Jaishanker. Boca Raton, FL: CRC Press, pp. 13–28.

Poulsen, Kevin. 2011. *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground*. New York: Crown Publishers.

Register of Copyrights. 2015. *Orphan Works and Mass Digitization*. Washington, D.C.: United States Copyright Office.

Rey, Sergio J. 2009. "Show Me the Code: Spatial Analysis and Open Source." *Journal of Geographical Systems*, Vol. 11, No. 2, pp. 191–207.

Romney, Marshall. 1995. “Computer Fraud—What Can Be Done about It?” *The CPA Journal*, Vol. 65, No. 5, pp. 30–32.

Ryan, Patrick S. 2004. “War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics.” *Virginia Journal of Law & Technology*, Vol. 9, No. 7, pp. 1–57.

Salus, Peter H. 1995. *Casting the Net: From ARPANET to Internet and Beyond*. Reading, MA: Addison-Wesley.

Santana, Mario. 2017. “Eliminating the Security Weakness of Linux and UNIX Operating Systems.” In *Computer and Information Security Handbook*, 3rd Edition, edited by John R. Vacca. Cambridge, MA: Elsevier.

Satapathy, C. 2000. “Impact of Cyber Vandalism on the Internet.” *Economic and Political Weekly*, Vol. 35, No. 13, pp. 1059–1061.

Schiller, Craig A., Jim Binkely, David Harley, Gadi Evron, Toni Bradley, Carsten Willems, and Michael Cross. 2007. *Botnets: The Killer Web App*. Burlington, MA: Syngress.

Schmitt, M. N. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, UK: Cambridge University Press.

Shabtai, Asaf, Yuval Elovici, and Lior Rokach. 2012. *A Survey of Data Leakage Detection and Prevention Solutions*. New York: Springer.

Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. 2013. *Introduction to Cyber Warfare: A Multidisciplinary Approach*. Waltham, MA: Elsevier.

Shaw, Thomas J. 2011. *Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists*. Chicago, IL: American Bar Association.

Skoudis, Ed, and Lenny Zeltser. 2003. *Malware: Fighting Malicious Code*. Upper Saddle River, NJ: Prentice Hall.

Slatalla, Michelle, and Joshua Quittner. 1995. *Masters of Deception: The Gang that Ruled Cyberspace*. New York: HarperCollins.

Spanos, Georgios, and Lefteris Angelis. 2016. “The Impact of Information Security Events to the Stock Market: A Systematic Literature Review.” *Computers & Security*, Vol. 58, pp. 216–229.

Stay, Ronald J. 1997. “Cryptic Controversy: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmermann.” *Georgia State University Law Review*, Vol. 13, No. 2, pp. 581–604.

Swartz, Aaron. 2015. *The Boy Who Could Change the World: The Writings of Aaron Swartz*. New York: The New Press.

Terasaki, Michael. 2014. “Do End User License Agreements Bind Normal People?” *Western State University Law Review*, Vol. 41, No. 2, pp. 467–489.

Tiirmaa-Klaar, Heli, Jan Gassen, Elmar Gerhards-Padilla, and Peter Martini. 2013. *Botnets*. New York: Springer.

Trautman, Lawrence. 2014. “Virtual Currencies Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox?” *Richmond Journal of Law & Technology*, Vol. 20, No. 4, pp. 1–108.

United Nations Office on Drugs and Crime. 2017. *World Drug Report 2017*. New York: United Nations.

United States Copyright Office. 2011. *Legal Issues in Mass Digitization: A Preliminary Analysis and Discussion Document*. Washington, D.C.: United States Copyright Office.

U.S. General Services Administration. “Continuous Diagnostics and Mitigation Program.” https://www.gsa.gov/technology/technology-products-services/it-security/continuous-diagnostics-mitigation-cdm-program

Wall, David S. 2001. *Crime and the Internet*. New York: Routledge.

Wenke Lee, Cliff Wang, and David Dagon. 2008. *Botnet Detection: Countering the Largest Security Threat*. New York: Springer.

Wolak, Janis, and David Finkelhor. 2016. *Sextortion: Findings from a Survey of 1,631 Victims.* Durham, NH: Crimes against Children Research Center.

Wolak, Janis, David Finkelhor, and Kimberly J. Mitchell. 2005. *Child Pornography Possessors Arrested in Internet-Related Crimes: Findings from the National Juvenile Online Victimization Study.* Washington, D.C.: Center for Missing and Exploited Children.

Woodward, John D., Jr., Nicholas M. Orlans, and Peter T. Higgins. 2003. *Biometrics*. Berkeley, CA: McGraw-Hill.

Yu, Shui. 2014. *Distributed Denial of Service Attack and Defense*. New York: Springer.

Zetter, Kim. 2014. *The Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers.

Index

Note: Page numbers in **bold** indicate the location of main entries.

About the Authors

NANCY E. MARION received her PhD in political science from the State University of New York, and completed her JD from the University of Akron in December 2019. She is currently a professor of Political Science with a joint appointment in Criminal Justice, serving as chair for both departments at the University of Akron. Her research revolves around the relationship of politics and criminal justice and how the two fields interact with each other. She is the author of many books and articles that examine the interplay of these fields.

JASON TWEDE received his PhD in Criminal Justice from the University of North Dakota and his JD from Thomas M. Cooley Law School. He currently works as an assistant professor in the Department of Sociology, Social Work, and Anthropology at Utah State University, Tooele campus. Prior to pursuing a career in academia, Jason worked as a prosecutor in Navajo County, Arizona. He worked on and prosecuted a wide array of criminal matters, though his work primarily focused on drug crimes—including drug interdiction and legal issues regarding medical marijuana—and arson.

Jason's background as a prosecutor has largely shaped his research. His primary focus has been on the history of prosecution in the United States, in particular the transition from private to public prosecution and the ramifications that transition has on the criminal justice system today. The research takes a critical approach, emphasizing how the interests of the socioeconomically advantaged have shaped this transition. His research has also included other legal transitions in the United States, such as the ongoing transition regarding the legalization of medical marijuana. This research likewise emphasizes how the interests of the socioeconomically advantaged have shaped this transition.