Cyber-Attacks – Trends, Patterns and Security Countermeasures

Article *in* Procedia Economics and Finance · December 2015

DOI: 10.1016/S2212-5671(15)01077-1

1 author:

Andreea Bendovschi
Bucharest Academy of Economic Studies
8 PUBLICATIONS **78** CITATIONS

SEE PROFILE

Cyber-attacks – trends, patterns and security countermeasures

Andreea Bendovschi

doi: 10.1016/S2212-5671(15)01077-1

Abstract

Technology is rapidly evolving in a world driven by social networks, online transactions, cloud computing and automated processes. But with the technological evolution comes the progress of cyber-crime, which continuously develops new attack types, tools and techniques that allow attackers to penetrate more complex or well-controlled environments, produce increased damage and even remain untraceable. The present article aims to get an overview of the cyber-crime as it is defined and revealed by specialized literature, international legislation and historical facts, and perform an analysis of attacks reported all around the world over the last three years in order to determine patterns and trends in cyber-crime. Based on the results of the analysis, the article presents countermeasures that companies may undertake in order to ensure improved security that would support in defending their business from attackers from an information security perspective.

Keywords: Cyber-crime, cyber-attack, cyber-security, controls

1. Introduction

In a world driven more and more by big data, social networks, online transactions, information stored or managed via internet and automated processes performed through the use of IT systems, information security and data privacy are permanently facing risks. With the development of new tools and techniques, cyber-crime is consistently increasing in terms of number of attacks and level of damage caused to its victims.

Developing new ways to gain unauthorized access to networks, programs and data, attackers

aim to compromise the confidentiality, integrity and availability of information, building their targets from single individuals to small or medium sized companies and even business giants. Every year seems to bring a bigger number of attacks overall, but also a bigger number of attacks defeating the security of extremely large companies, thus affecting the information security, business continuity and customers' trust. The increasing trend has reached new peaks in 2014, universally known as "the year of cyber-attacks", but the authors believe this is not to be the apogee unless countermeasures are taken at a global scale. This article has the purpose of revealing results, trends and patterns noted by the authors through the analysis of the attacks reported in the last three years, and to present countermeasures that should be taken as for supporting the improvement of security and the decrease of world-wide cyber-crime. The article is structured in three main parts: it begins by presenting the general view of cyber-crime from the perspective of specialized literature, international law, as well as historical facts and continues through revealing the main results and interpretation of the study performed over the last three years' reported attacks. It ends by drawing some of the main countermeasures that companies may undertake in order to ensure improvement of controls covering the information confidentiality, integrity and availability, while decreasing the security breaches.

2. Literature review

Cyber-attacks become more and more a daily reality for both companies of all sizes as well as single individuals, however yet little is universally known about cyber-crime. M. Uma and G. Padmavathi (2013) outline that there is a general lack of understanding of the different types of attacks, characteristics and possible results, which may pose an obstacle in trying to defend the information security.

Several definitions of the terms cyber-attack, cyber-crime, etc. can be found among the international literature, all having in common the aim to compromise the confidentiality, integrity

and availability of data. The technological evolution also brings along the progress of cyber-crime, thus new ways to perform attacks, reach to even harder to penetrate targets and remain untracked are developed continuously. However, traditional cyber threats remain the source of the most common attacks. Various types of attacks have been defined and studied among the international literature:

- Man in the middle attack occurs when the attacker interferes between the two communication ends, thus every message sent from source A to source B reaches the attacker before reaching its destination. The risks further posed by this type of attack comprise of unauthorised access to sensitive information or possibilities to alter the information/message that reaches the destination by the attacker;
- Brute force attack comprises of repeated attempts to gain access to protected information (e.g. passwords, encryption, etc.) until the correct key is found, and information can thus be reached;
- DDoS (Distributed Denial of Service) is a type of attack that compromises the availability of data, in the way that the attacker floods the victim (e.g. server) with commands, thus becoming inoperable;
- Malware is a generic term describing types of malicious software, used by the attacker to compromise the confidentiality, availability and integrity of data. Most common types of malware are: viruses, worms, trojans, spyware, ransomware, adware and scareware/rogware;
- Phishing is a technique aiming to steal private information from users through masquerading as a trustful source (e.g. website);
- Social engineering is the general term that describes techniques used to gain unauthorized access to information through human interaction.

PriceWaterhouseCooper's study, The Global State of Information Security 2015, outlines the

fact that cyber-crime has developed to an extent that brings over 117,000 attacks per day.

3. Research Methodology

The study commenced with an attentive review of cyber-crime's current position, through the review of specialised international literature, including legal aspects, and analysis of the last years' major events. The aim was to gain a general overview of the cyber-attacks from all over the world, understand the means of operating and potential impact upon businesses or individuals, as well as the countermeasures to be taken as for addressing the risks. The research was based on attacks identified and traced among the last three years. Given the huge number of cyber-attacks undertaken on a daily basis all around the world, as well as the limited information companies usually display when they are the victim of cyber-crime and the fact that some attacks are hard to be traced, it was impossible for the authors to gain a complete set of data for analysis purposes. However, the study was based on the information resulted from aggregating data regarding attacks detected and traced throughout the last three years, collected from news and attacks history, as well as from reports and surveys issued by globally major market players in security consulting and anti-malware services, thus reaching a population of over 15 million attacks.

4. Study results

4.1. General results

The study was based on a population of over 15 million attacks, collected throughout news and events, as well as reported by major players in the industry of security and consulting: Cenzic, CISCO, FBI (Federal Bureau of Investigations), FireEye, Kaspersky, McAfee, Mandiant, Sophos, Syumantec, Verizon, PriceWaterhouseCoopers, hackmageddon.com.

McAffee Labs' report, Threats Predictions 2015, supports the idea that cyber-attack will

pursue an increasing trend, outlining the expectancy of increased espionage and cyber-warfare, also strengthened by hackers' improved strategies and tools for hiding their identity/location and obtain sensitive data. According to the report, 'Attacks on Internet of Things devices will increase rapidly due to hypergrowth in the number of connected objects, poor security hygiene, and the high value of data on IoT devices', also forecasting an estimated number of 50 billion of devices to be connected to the internet by 2019. The results outline the fact that attackers continuously develop new ways to exploit networks, programs and data. One other trend that has been noted is the continuous increase of mobile attacks from one year to another.

4.2. Main drivers

An interesting fact that the study reveals is that, looking at the root-cause of the security breaches, less than 50% of the cases are due to criminal intended attacks, the causes being split between three factors: the intended attack, the human error and the system vulnerabilities. The results outline the fact that when an attack succeeds, it is only partly due to the attacker's skills and knowledge, and also due to vulnerabilities from the victim's side – that is, faulty programs, human errors, insufficient level of controls to ensure information security. In 2013, Cenzic company has detected one or more major security vulnerabilities in 96% of the analysed applications, according to 2014 Application Vulnerability Trends Report, with a median of 14 vulnerabilities per application.

4.3. Attacks

Throughout the study it was hard to determine the exact number or percentage of different attack types, however the most common attacks are: denial of service, malicious codes, viruses, worms and trojans, malware, malicious insiders, stolen devices, phishing and social engineering, web-based attacks. Nevertheless, the results could easily be split into for

categories, depending on the objective of the attack: cyber-crime, cyber espionage, cyber war and hacktivism.

4.4. Distribution

The study revealed the fact that companies of various sizes and business sectors have been the victims of cyber-attacks in the last three years. Regardless of the entity's size, all areas, from the public sector (Government, Law Enforcement, Education, Healthcare) and Non-profit organisations to private companies from Finance, Media, Online services, Tourism, Telco, Retail, Education, Automotive, Security, Energy & Utilities, Food & Beverage, Internet and online services sectors are targeted by cyber-attacks. With regards to the geographical split of the attacks, the study focused on two perspectives: the geographic source of the attacks, as well as the destination. The results reveal that the most common attack sources are: USA, Russia, The Netherlands, Germany, the United Kingdom, Ukraine, France, Vietnam, Canada, Romania and others. At the same time, the most frequent victims are located in: USA, Russia, the United Kingdom, Germany, Italy, France, the Netherlands, and others.

4.5. Impact

With regards to the impact that cyber-attacks have upon their victims, it is hard, if not impossible, to quantify the exact costs that organisations required as for recovering their business, customers' trust and image, especially considering that companies do not always reveal all information to the public; however, the results show that the impact of cyber-attacks most often concern loss of information, business disruption, revenue loss and equipment damage. The most common types of attacks granted unauthorised access to information comprising of: full names, birth dates, personal IDs, full addresses, medical records, phone numbers, financial data, e-mail addresses, credentials (usernames, passwords), and insurance information.

4.6. Correlations, trends and patterns

The study revealed interesting results, trends and patterns. First of all, the results outline a relative correlation between the business sector and the types of attacks; thus, cyber espionage is most likely to be aiming Government, Media and Law Enforcement sectors, and quite unlikely to target other business sectors (Retail, Telco, Online Services, etc.). The results for the last 3 years outline a relatively strong correlation between the types of attacks and industries, as presented in Figure 1. The correlation shows that while the public sector (government, law enforcement, education, etc.) is most likely the target of cyber espionage, cyber war and hacktivism techniques, cyber-crime targets all business sectors.

The results also show that attacks are not totally due to outside hackers, but split between them and company-related factors (partners, current or former employees, management, etc.). The results may also draw a few trends, making the authors believe that unauthorised physical access continuously loses ground against unauthorised logical access to data. Also, it was noted a continuous increase in the mobile attacks, which authors believe to be natural considering the spread of smartphones, which may prove to be an easy target due to almost permanent connection to the internet, use of a series of social network and other applications, as well as the facts that they are barely switched off and contain/retain a lot of personal information (from name, phone number and location to the most recent networks the device was connected to, etc.).

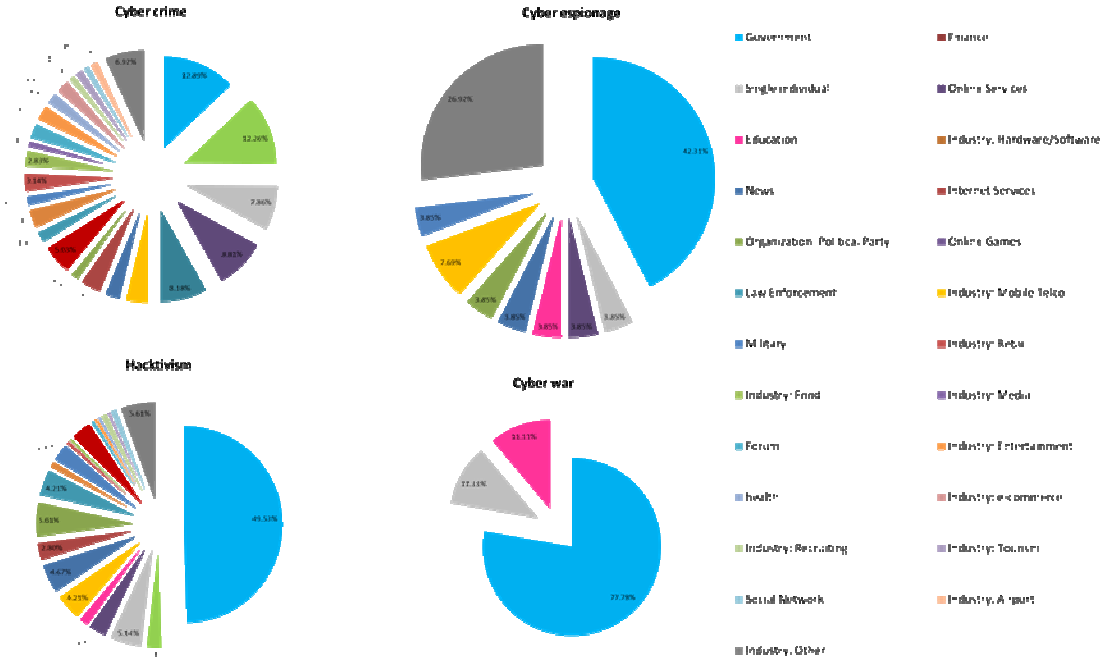

Fig. 1: Cyber-attacks per industry sector

5. Security countermeasures

5.1. External

Nowadays, a series of non-profit organisations are fighting against cyber-attacks, such as Secure Domain Foundation (SDF) or the International Association of Cyber-crime Prevention (IACP), trying to make the public (companies and individuals) aware of risks, attacks, how they can be exposed to the cyber-crime, and how they can defend themselves against attacks. Apart from the non-profit organisations, Google itself has also recently started developing its own team, called Project Zero, meant to analyse bugs and vulnerabilities in their own as well as other companies' codes in order to take all necessary measures as for improving the software products so cyber-attack risk is mitigated.

The increasing trend of cyber-attacks has also reached the eyes of financial institutions. AXA Corporate Solutions Company is just one of the financial companies that have launched an insurance product covering costs needed to recover after a cyber-attack, viruses, errors or accidental events. In addition, the company also launched a product dedicated to analyse, assess and support mitigate clients' cyber risks.

One essential aspect when discussing cyber-crime and security is the legal aspect. Laws and regulations are continuously developed to prevent or limit the cyber-crime, however the sensitivity of the subject is given by the fact that each set of laws and regulations are geographically limited to a certain state/region/etc. in spite of the internet access, which is world-wide and internationally by definition, connecting people from all around the world with no boundaries.

5.2. Internal

Continuous risk assessment

There are no two companies alike. That is why each company, depending on its size, geographical setup, business operating sector, etc. has its own risk profile. Each company should perform a series of steps required as prerequisites to implementing security controls, covering identification of threats, vulnerability, risks and design and implementation of security controls addressing these risks.

IT environment's health

Companies should make sure all equipment (hardware and software), including protection software (e.g. antivirus programs) is always up to date, latest patches are installed, and no exceptions occur. Also, it is essential for companies to ensure there is an agreement in place for third party provided software covering the maintenance and upgrade services.

Authentication

Depending on the risk assessment, access to the company's programs and data may be protected solely by a password. However, especially for remote access or web-based applications, it may be recommended to use more complex authentication means - combining at least two of the following: something you know (e.g. password), something you have (e.g. random PIN generating device), something you are (e.g. biometric authentication).

Internal commitment and responsibility

Company-wide awareness is essential, considering that vulnerabilities and risks are more often than expected caused by security breaches created (even unintended) by the company's own staff. Thus, documenting the processes and controls in place into a formalised set of policies and procedures, ensuring a clear and concise way to present the information as well as enforcing the awareness and commitment of staff may support improving and maintaining the information security.

Access to information

Companies should ensure access is appropriately restricted and timely terminated for leavers, contractors, auditors or other third parties that have previously required connection to the company's network. A large range of controls may address these risks, from manual controls (e.g. periodic review of all user access rights) to automated controls may ensure that (e.g. automatically disabling domain accounts that have not connected to the network for a certain period of time).

Data retention

The simplest way of avoiding information security to be compromised is to remove all data that is no longer required for daily business purposes. Archiving and retention of data should ensure data is kept as long as needed on a dedicated environment (back-up servers, dedicated archives, etc.), and removed from the company's network, thus limiting the risk of unauthorised access to sensitive information, especially considering that the study revealed the fact that more than 20% of the stolen information was data the victim had no clue it was stored on the company's network.

Other security controls

Depending on the risks to be addressed, several controls may be implemented in order to ensure the confidentiality, integrity and availability of data. Controls may differ from one company to another, and may be classified in:

- Preventive controls – security controls aiming to prevent any threat (e.g. restricting access to the company's network, programs and data may prevent unauthorised access);
- Detective controls – controls aiming to detect any threat to the information security (e.g. even if unauthorised access was reached, intrusion detection system monitors the network traffic and identifies the suspicious access);
- Corrective controls – security controls aiming to correct irregularities identified (e.g. business recovery after an attack).

Independent reviews

The technological evolution involves more and more daily operations/processes to be managed through information systems requiring the use of the internet. But together with the technological evolution comes the development of existing threats and related risks, as well as possible controls to implement as for addressing them. Thus, having independent security

reviews covering different areas (e.g. internet banking system certification and audit, penetration tests, etc.) may help detect security breaches and support the implementation or improvement of security controls.

6. Conclusions

There is great room for improvement in the world's fight against cyber-crime. M. Uma and G. Padmavathi (2013) state that there is a general lack of understanding attacks (types, characteristics and potential impact), thus the world is facing a huge problem in ensuring proper security of information. The authors believe that the first thing to do in order to handle the problem of increasing cyber-crime is a world-wide awareness, from an individual level to company perspective, of what lays in the cyber world. One other main obstacle is probably the legal perspective, in the sense that even though each state or region has its own set of laws and regulation governing the invasion of data privacy and theft, the internet is an international tool for attackers, thus the only way to defeat the cyber-crime is for authorities to think and act at a global level, thus supporting the rights and safety of citizens of the entire world. Last but not least, it is the responsibility of each individual, company or authority to ensure a certain level of security, personally assessed and developed, in order to support the information security and data privacy, as it is the right of every individual, company or authority to decide what and how they retain, manage and share their data.

Further directions of the study will comprise of closely following the evolution and trends of cyber-crime, as well as of countermeasures, especially focusing on the universal awareness regarding cyber-crime and regulatory decisions and facts meant to support the cyber-security.

Acknowledgements

This paper was co-financed from the European Social Fund, through the Sectorial Operational Programme Human Resources Development 2007-2013, project number POSDRU/159/1.5/S/138907 "Excellence in scientific interdisciplinary research, doctoral and postdoctoral, in the economic, social and medical fields -EXCELIS", coordinator The Bucharest University of Economic Studies.

References

Akhgar, S., Yates, B. (2013) Strategic Intelligence Management, 1st Edition, Butterworth-Heinemann, 9780124071919, 56-255.

Axa Corporate Solutions official web-site, description available at http://www.axa-corporatesolutions.com (website visited on July 15, 2014).

Cenzic (2014) Cenzic, Application Vulnerability Trends Report: 2014, description available at: www.cenzic.com (website visited on January 03, 2015).

CISCO (2014) CISCO 2014 Annual Security Report, description available at: www.cisco.com (website visited on January 04, 2015).

CISCO (2013), CISCO 2013 Annual Security Report, description available at: www.cisco.com (website visited on January 04, 2015).

CISCO (2012), CISCO 2012 Annual Security Report, description available at: www.cisco.com (website visited on January 04, 2015).

Google Project Zero blog, description available at: http://googleprojectzero.blogspot.co.uk/2014/ 07/announcing-project-zero.html (website visited on January 10, 2015).

Federal Bureau of Investigation (2013), 2013 Internet Crime Report, description available at: http://www.fbi.gov/stats-services/publications (website visited on January 04, 2015).

Federal Bureau of Investigation (2012), 2012 Internet Crime Report, description available at: http://www.fbi.gov/stats-services/publications (website visited on January 04, 2015).

Federal Bureau of Investigation (2011), 2011 Internet Crime Report, description available at: http://www.fbi.gov/stats-services/publications (website visited on January 04, 2015).

FireEye company (2012), FireEye advanced threat report: 2013, description available at: http://fireeye.com (website visited on January 04, 2015).

FireEye company (2012), FireEye advanced threat report: 2012, description available at: http://fireeye.com (website visited on January 04, 2015).

FireEye company (2011), FireEye advanced threat report: 2011, description available at: http://fireeye.com (website visited on January 04, 2015).

Kaspersky (2013), Kaspersky Security Bulletin 2013, descrption available at: http://securelist.com (website visited on January 04, 2015).

Kaspersky (2012) Kaspersky Security Bulletin 2012, description available at: http://securelist.com (website visited on January 04, 2015).

Kaspersky (2011) Kaspersky Security Bulletin 2011, description available at: http://securelist.com (website visited on January 04, 2015).

Mandiant company (2014) 2014 Threat report: Beyond the breach, description available at: http://www.mandiant.com (website visited on January 04, 2015).

McAfee Labs (2014) Threats Predictions 2015, description available at: http://mcaffee.com (website visited on January 04, 2015).

McAfee Labs (2013) Threats Predictions 2014, description available at: http://mcaffee.com (website visited on January 04, 2015).

McAfee Labs (2012) Threats Predictions 2013, description available at: http://mcaffee.com (website visited on January 04, 2015).

MIT Geospatial Data Centre (2013), Cyber security and human psychology, description available at: http://cybersecurity.mit.edu/2013/11/cyber-security-and-humanpsychology (website visited on July 15, 2014).

PriceWaterhouseCoopers, InfoSecurity (2014) 2014 Information Security Breaches Survey, descrption available at: http://www.pwc.co.uk (website visited on January 10, 2015).

PriceWaterhouseCoopers, InfoSecurity (2013) 2013 Information Security Breaches Survey, description available at: http://www.pwc.co.uk (website visited on January 09, 2015).

PriceWaterhouseCoopers, InfoSecurity (2012) 2012 Information Security Breaches Survey, description available at: http://www.pwc.co.uk (website visited on January 09, 2015).

Sophos company (2014) Security Threat Report 2014, descrption available at: http://sophos.com (website visited on January 04, 2015).

Sophos company (2013) Security Threat Report 2013, description available at: http://sophos.com (website visited on January 04, 2015).

Sophos company (2012) Security Threat Report 2012, descrption available at: http://sophos.com (website visited on January 04, 2015).

Symantec company (2011) Internet Security Threat Report 2011, description available at: http://symantec.com (website visited on January 04, 2015).

Symantec company (2012) Internet Security Threat Report 2012, description available at: http://symantec.com (website visited on January 04, 2015).

Symantec company (2013) Internet Security Threat Report 2013, description available at: http://symantec.com (website visited on January 04, 2015).

Symantec company (2014) Internet Security Threat Report 2014, description available at: http://symantec.com (website visited on January 04, 2015).

Uma, M., Padmavathi, G. (2013) A survey on various cyber-attacks and their classification, International Journal of Network Security, 15, 5, 390-396.

Verizon (2012) 2012 Data breach investigation report, description available at: http://verizon.com/enterprise/securityblog (website visited on January 04, 2015).

Verizon (2013) 2013 Data breach investigation report, description available at: http://verizon.com/enterprise/securityblog (website visited on January 04, 2015).

Verizon (2014) 2014 Data breach investigation report, description available at: http://verizon.com/enterprise/securityblog (website visited on January 04, 2015).

Wall, D. (2007) Cybercrime: The Transformation of Crime in the Information Age, Polity Press 2007, ISBN: 0-74562735-8, 8-58.

Wang, P., Liu, J. (2014) Threat analysis of cyber-attacks with Attack, Journal of Information Hiding and Multimedia Signal Processing, 5, 4, 778:787.

Westerman, G. (2013) Your Business Is Never Too Small For A Cyber-attack, Here's How To Protect Yourself, Forbes, descriptoin available at: http://www.forbes.com/sites/forbesleadershipforum/ 2013/05/13/your-business-is-never-too-small-for-a-cyber-attack-heres-how-to-protect-yourself/ (website visited on February 02, 2015).

Yar, M. (2013) Cybercrime and society, Sage Publications 2013, Second Edition, 978-1-44620-193-0, 9-67.