FROM CYBER THREATS TO CYBER-CRIME

Stefan Iovan [1*]
Alina-Anabela Iovan [2]

ABSTRACT

*Cyber-attacks and / or on the web arose with the advent of the Internet. They use a variety of malware software. Phishing attacks and spam remain the cyber threats companies are facing most frequently. At the same time the volume of malware and spam attacks have increased substantially in the past years. The threat of cyber-crime is a daily reality for companies and making the challenges dynamic and continuous. This means that the CEOs (**C**hief **E**xecutive **O**fficers) and top management must include FDA (**F**orensic **D**ata **A**nalytics) as a critical component in their risk management and compliance. The need for these investments is strengthened by the current regulatory environment and market reaction to situations of alleged fraud, bribery and cyber-attacks in the corporate environment. The fact that these attacks will not disappear is given by the reasons behind them, which is that are closely related to people's thirst for power, fame and wealth. The paper aims to present relevant issues, statistics and considerations on this phenomenon - crime / cybercrime and / or cyber. In the end of the paper we present a few issues of the last level that was reached - in cyber war.*

KEYWORDS: *cyber-attacks, cyber war, cyber mercenaries, ransomware, active and proactive actions*

1. INTRODUCTION

Today more and more companies, businesses, government agencies and non-governmental organizations become victims of cyber attacks [1]. According to a survey, 91% of organizations surveyed have experienced a cyber attack at least once in the last 12 months, while 9% were victims of attacks target predefined - activity carefully planned in advance in order infect the network infrastructure of a specific organization. These are just estimated information companies. The widespread use of digital devices in business activity has created ideal conditions for the development and launch cyber espionage malware that can steal company data.

[1]* corresponding author, Associate Professor PhD, Computer Science Department, West University Timisoara, Romania, stefan.iovan@infofer.ro
[2] Engineer, Railway Informatics SA, Software Development Department, Bucharest, Romania, alina.iovan@infofer.ro

2. THE THREATS FOR COMPANIES

Potential Cyber Threats (informatics) is so large, that malware can replace almost completely in the near future sources inside the company and other classical techniques for gathering information [2]. The main findings of recent years are:

- were disclosed spyware attacks aimed at government organizations;
- most cyber incidents were aimed at stealing information;
- attacks identified to target contractors in order to reach large organizations;
- there is a new actor entering the stage of APT (***A**dvanced **P**ersistent **T**hreat*): cyber mercenaries who carry out cyber espionage operations on demand;
- ransomware kind of attack (malicious software that prevent access to files or even entire infected system, until is payee the 'reward').

2.1. Parties concerned and the objectives of attackers

In 2014 it was discovered important new information about spyware attacks, which have been linked directly or indirectly to the activities of various government agencies. Other important actors on stage to address cyber threats companies were companies who used cybercriminals to gain access to competitor's networks [1, 2]. Cybercriminals subcontracted operations were performed aimed, in general, as information thefts. Other attacks were based on sabotage - use malware to wipe data or lock infrastructure operations.

Some special type programs, like Trojans virus were able to steal money through online banking systems. Cyber criminals can also compromise the websites of companies and redirect visitors to malware resources, in order to damage a company's reputation. Financial losses can be caused by DDoS attacks that can shut down the public website of a company for several days. In such cases, customers can search for a company more reliable, leading to long-term financial losses.

Mass distribution of malware can affect any company, even a small commercial organization, resulting in loss of money and intellectual property. Cybercriminals are improving continuously the malware using approaches and the unconventional solutions, the so-called "encryptions," and "shredders" that spread like a plague in a corporate environment, an army of zombies devouring all available resources web servers and network data transfer.

Also, 2014 was the first case of attack against supply chains - because they were not able to reach large organizations, cybercriminals have targeted their weakness, firstly aiming contractors, as in attacks Icefog. '*Icefog*' is an APT group attacking targets in South Korea and Japan, focusing on supply chains of Western companies. The operation began in 2011 and has evolved over the past years. An Icefog group reveals new cyber mercenaries that are hired to conduct operations such as hit & run (*'attack and run'*) kinds.

2.2. Emergence of cyber 'mercenaries'

Over the past years, security experts have discovered APT groups large and "noisy" all over the world, attacking a large number of organizations in almost all sectors. They

remained in the compromised network for weeks or even months to steal any shred of information they could get. However, this approach has increasingly unlikely to go unnoticed for long, reducing their chances of success. Therefore, there is a new trend in developing both small groups such as "hit-and-run" which attack with surgical precision.

They seem to know very well what they need from the victims. Basically, this type of attack comes, knows what will steal and goes away. Experts have called 'cyber mercenary' - an organized group of people engaged in cyber espionage or sabotage on the request if a payer, following orders.

Icefog, which was discovered in autumn 2013 seems to be a clear example of this - an APT campaign in search of data specifically required. Manual analysis of information stored on corporate networks has been achieved through technologies allowing remote access integrated into malware from infected computers. Subsequently, cybercriminals have selected and copied documents they wanted. Analysts and experts expect this trend to grow in the future and that several small groups of cyber mercenaries to be available for contracting operations in order to perform precise type of hit-and-run attacks.

2.3. Consequences of disclosure information related to Governmental organizations

Great revelations of 2013 and 2014 could lead to a kind of globalization and greater interest for the creation of national equivalent of global services. These new software products and services nationally supplied by local producers can not have the same quality as those of larger international companies. Survey cyber attacks suggests that the more a software developer is smaller and less well known, the more vulnerabilities will be identified in the code of that software. As a result, the predefined target attacks have become simpler and more efficient.

3. MAIN CYBER THREATS

Cyber attacks and/or use a variety of cyber malware. Phishing attacks and spam remain the cyber threats facing companies most frequently. At the same time, the volume of malware and spam attacks has increased substantially in 2014 to 2013. These are the findings of the survey study [3] conducted by B2B International. Although the data is old they are meaningful to make comparisons and seeing the evolution relative to the topic being discussed.

Approximately 68% of respondents said that their companies were targets of attacks by viruses, worms, spyware and other malware. In 2012, this number was lower by 6% (62%). The volume of spam attacks has increased considerably, affecting 61% of companies, compared to 41% in 2012. Phishing attacks were launched against 36% of companies with 1% less than in 2012. Beside that, phishing remains one of the most prevalent threats in external attacks against corporations. Companies in South America were most frequently attacked: 72% of respondents in the region said that viruses and spyware are the most serious external threats.

Russian companies were also attacked frequently, accounting for 71% of these incidents. In Japan, companies have experienced the least with this problem, only 47% of respondents being the target of malicious attacks. The largest amount of spam was

recorded in companies in North America and Russia (in 69% and 67% of cases). Companies that face the least with spam are the Middle East (55%) and Japan (42%). Companies in North America were faced with phishing attacks more frequently than in other regions (51%), followed by companies in Asia Pacific (46%). Companies with the lowest rate of phishing attacks are from Russia, Japan and South American countries (on an average of 26%).

Malware attacks are in fact the main cause behind the severe leakage of confidential data: 22% of companies globally and 24% in Eastern Europe had leaked database for this type of attacks. Most often, these injuries occur among small and medium enterprises (23%), whereas large companies are attacked less frequently (17%). Data leaks occur less frequently as a result of phishing attacks, an average of only 5% of companies facing such events globally and 4% in Eastern Europe. However, the percentage of large companies that lost their data due to phishing attacks is somehow higher (6%) than the number of SMEs in the same situation (5%). The number of cyber threats is constantly increasing. They are discovered more than 200,000 new malware samples every day. This causes companies to pay more attention to security, especially after confronting a cyber incident.

However, according to the study, only 68% of companies have implemented a comprehensive anti-malware (anti-virus and anti-spyware). This is a small improvement over the figure of 51% recorded in 2012. Thus, companies are changing security situation, more and more companies moving towards complex security solutions. The variety of attacks launched against companies indicates that their need for a specialized security solution capable of effectively counter cyber threats dangerous. For example, Kaspersky Endpoint Security for Business (KESB) [4] is a solution that protects infrastructures IT (Information Technology) companies.

In addition to modern technologies antivirus, it includes components that protect against attacks targeted predefined, phishing and spam. Interacting regularly with cloud service and using heuristic detection technology complex and blocking threats, KESB solution provides robust security infrastructure for any type of company [4].

4. DATA ANALYSIS FOR CYBERCRIME CASES

Cyber attacks and insider threats, malicious generated including employees who evade, manipulate or destroy data, the risk is the highest growth rate, leading investment solutions FDA, according to edition 2016 study [5]. The study [5] was conducted globally among the 665 executives from nine industries, including financial services, pharmaceutical and healthcare, manufacturing, energy and utilities.

Researching the use of tools of data analysis to investigate the incidents and to manage risks, the study found that the risk of fraud domestic ranks first position with 77%, while risk-intrusion system or the internal threat ranks second with 70%. 69% of respondents say they have made efforts to be able to update their anti-fraud procedures, including the use of data analysis tools of cybercrime (FDA). It noted here that this figure increases to 74% for managers in top management positions. Of the respondents who say that pressures from regulations are the main reason for improving procedures, those holding

top managerial positions proved most concerned that the limitations and constraints imposed legal requirements are becoming more widespread and harder.

The threat of cyber crime is a daily reality for companies and challenging dynamic and continuous. This means that the CEOs and top management must include FDA (Forensic Data Analytics) as a critical component in their risk management and compliance. The need for these investments is strengthened by the current regulatory environment and market reaction to situations of alleged fraud, bribery and cyber attacks in the corporate environment.

4.1. Increase investment in FDA

As only 55% of respondents claim that the funds allocated FDA in their companies enough - value down from 64% in the survey in 2014 - is not surprising that three out of five respondents said that they intend to spend more on such IT tools in the next two years. Studying the reasons for the increase of these investments, first invoked was in response to increasing cyber crime, followed by the increasing pressure exerted by the legislature with 53% and 43% respectively. It also changes and the implementation of instruments FDA, 63% of respondents stating that invest at least half of the budget FDA proactive in monitoring activities.

4.2. Increase use of FDA

Responding to increased risk of advanced instruments FDA has become a norm, new technologies and new monitoring techniques are more widely used to support companies in managing current and future risks related to fraud and cyber crime. Maturing corporate efforts in the FDA is increasingly obvious, if we look at increasing sophistication in using the data. 75% of respondents routinely examines a wide range of structured and unstructured data, allowing them to obtain a holistic picture of the universe own risk. Given the pressure faced by organizations in terms of fraud prevention, it is not surprising that most respondents effort is growing in support of proactive initiatives.

Monitoring and surveillance programs that use FDA tools can help organizations strengthen their compliance programs with legislative requirements, improving corporate culture and fostering increased confidence in the regulators and the other actors involved in the smooth running of the company. The experience that organizations have in the region, is based on investigations with a varied and complex casuistry conducted using advanced computer resources and internationally certified, which ensures flexibility and scalability required to customer requirements.

4.3. Manturing of FDA leads to possitive results

Results of the study [5] shows that there are remarkable similarities between the organizations reported positive results from efforts related to the adoption FDA instruments such as:

- Greater share of budgets allocated FDA compliance and antifraud;
- The adoption of sophisticated data analysis tools, including social media monitoring, web and visualize environmental data in a mix of illegal activity or to identify patterns and trends of fraud;
- Incorporation of larger volumes of data and a larger variety of data sources (both structured and unstructured how).

Nowadays, the tools become indispensable FDA for the proactive management of risk. Organizations must recognize the role that FDA instruments can play not only in investigations of reactive but also proactive in the work of supervision, compliance and response efforts in anti-fraud and anti-cyber crime.

5. LOSS OF DATA FROM THE COMPUTER

Most users that the data they store on their devices are more important than the computer itself. According to a survey [6] conducted in the summer of 2013 by B2B International, 59% of users believe that their photos and documents are even more valuable than an expensive computer. However, if a malicious attack, over 50% of them stated that they were unable to recover all the lost data.

What is more valuable: an expensive computer or a first photograph of a child stored on your hard drive? A laptop or emails shared with loved ones stored in its memory? The next-generation tablet or videos from a meeting with dear friends? Most respondents unanimously elected - personal information is worth more than any device, no matter how expensive it is. Unfortunately, people often lose valuable information: according to the survey, one in five malware attacks ending with the loss of personal data. 61% of users who were attacked were not able to recover all the lost information.

For cybercriminals, personal data is an asset that can be sold: they can steal valuable information for use other fraudulent actions, such as to get control over accounts online banking user or to block access to sensitive information, demanding a ransom in exchange for their recovery (ransomware attacks). The widespread use of mobile devices has aggravated the situation: each new personal smartphone or tablet gives criminals a way to further attack. Although the variety and number of cyber threats are growing personal information can be kept secure using reliable security solutions.

5.1. What really matters?

For many years, they are developed technologies that effectively combat cyber threats. Throughout these years, the efforts of teams of experts have enhanced their capacity proven security products not only to detect all types of malware and to protect users' personal data and bring him his secure access to online services. Solutions that protect multiple devices with different operating systems were developed specifically to accomplish these tasks.

These solutions combine the best technology tested over time, developed by companies to combat cyber threats. Whatever type of device and the operations performed with it - transferring money to family or friends through an online payment system from a PC, download a package of new musical instruments virtual Mac installation of a popular

game a new Android smartphone or tablet - security solutions provide equally high-quality protection for digital assets stored on all devices.

The products integrate a number of advanced technologies that fight against malware, phishing, spam, financial attacks, attacks aimed at children and the theft of personal data or devices. Besides protecting extremely effective against cyber threats, security solution has another valuable feature - it can save you time when you need updated license for each device. For example, all the solutions contained in the package [7] are activated and updated less than one license, and users can choose the exact combination and number of devices to be protected. In addition, when the user wants to replace a device with a new one, existing license can be transferred to the new device.

6. CYBER WAR

Wars occurred since the beginning of the world. Cyber attacks have occurred with the advent of the Internet. The fact that these attacks will not disappear is because the reasons behind them are closely related to people's thirst for power, fame and wealth. We can draw parallels between physical and cyber wars. Therefore, it may not be a bad idea to learn a few things about war strategies of one of the greatest works ever written about war - Art of War by Sun Tzu.

Written 2,500 years ago by the famous Chinese general, strategist and philosopher Sun Tzu, the book is a reference for many business leaders. This is a masterpiece containing valuable information about the ways in which the business area leaders overcome their competitors. The book also can be a benchmark for organizations that try to take the lead in cybernetics. Here are some quotes from Sun Tzu that every CIO should know by heart:

Know your enemy and know yourself; in a hundred battles you will not be exposed to any dangers. If you do not know your defensive cyber capabilities will be needed to discover quickly. But this is not enough. It is essential to have accurate and updated information about the attacker. In the context of cyber attacks, acts it translates that information is of extreme importance.

In a recent summit at the White House, White House Cyber Security Summit, US President called for speedier exchange of information on threats in the public and private sectors and better coordination in the fight against cyber attacks. This is good advice which should give it more attention. Independent organizations rarely see the bigger picture behind the cyber attacks. They are so absorbed by actions to stop an attack of efficient IT service costs and decrease downtime. The failure to share information with other companies allows hackers to learn from each attack, to adjust their tactics and apply new techniques on new targets.

Sharing information sharing related threats related to the attack contexts. This is essential because it allows companies to understand the three major issues: the techniques used by hackers, the common characteristics of companies that have been victims of an attack and how hackers behave once they compromise a company. Theses three information’s helps immensely in IT security teams to identify and block new attacks in a more efficient manner, thereby increasing security for companies and consumers. For this reason, Fortinet founded Cyber Threat Alliance, an initiative which aims to generate a framework

for sharing information related to cyber attacks with other security technology vendors worldwide.

A skillful fighter is one who not only wins, but excels in winning with ease. The basic purpose of a company is to generate profit. A cyber attack succeeded not only affects your finances and reputation, but they also require subsequent expenditure. To mitigate the final impact, companies need to clear the attacks in a cost effective manner. At the summit on cyber security, the US president called for companies to invest more in security technologies.

Technology has changed radically in recent decades. Networks have become incredibly complex, while the emergence of mobile and agile infrastructure, cloud, hampered them safe administration. Old security technologies can not cope with the environment and must be replaced. Technology is constantly evolving to keep pace with the hackers. While we already have the ability to organize various facets of cyber security of the future will be able to do more interesting things. In a few years, behavioral analysis will become common practice in security devices. Development of information science will allow IT security teams to keep information away from the vicinity of the big time, thus increasing companies' ability to predict attacks before they are launched.

If the enemy will strengthen the front line, we will weaken the rear; whether it will strengthen the home front, we will weaken the forefront; that will strengthen the left, we will weaken the right; that will strengthen the right, and we will weaken the left. If all these parties will strengthen, we weaken each. This quote reminds realities faced by those who occupy the CIO every day. Securing a company is a tough job, because hackers can seep through the smallest gaps.

One of the major drawbacks facing companies today is associated with low visibility applications, users and network services. The situation is worsening due to applications increasingly more stored in virtual environments. In addition, traffic rather dominant migrating from east to west (in the Data Centre) than from north to south (outside the boundary of the Data Centre).

New technologies are being developed to improve the visibility of software defined a new world where applications can be inspected in the virtual environment. Varied as these technologies are introduced on the market, those who occupy CIO is used to understand how each of these technologies and learn to organize information effectively. Otherwise, the really important information will be overshadowed by false alarms.

New technologies are being developed to improve the visibility of software defined a new world where applications can be inspected in the virtual environment. Varied as these technologies are introduced on the market, those who occupy CIO is used to understand how each of these technologies and learn to organize information effectively. Otherwise, the really important information will be overshadowed by false alarms.

Worldwide, companies that continuously train users using well-developed awareness programs start to notice a decrease in ordinary social engineering attacks such as spear-phishing attack type. User’s education and awareness are two of the most effective areas that companies can develop to lower risk on cyber secure. Applying the above tips we security strategy, we improve how the company responds to cyber attacks.

7. RECOMMENDATIONS AND SOLUTIONS SECURITY MATTERS

One very important thing that should not be overlooked is securing computers and personal devices - otherwise, cybercriminals can take the time to attack them. Internet users must check and, if necessary, to update their computer security, smart phones and tablets [8]. Inadequate security of computers and mobile devices facilitate attacks against users and criminals stealing data such as information on credit cards or access data services or paying online stores. In this regard, security breaches uncovered in outdated programs or operating systems and applications handled on mobile devices are the gateway ideal for attackers. Users should see the recommendations as an opportunity to secure their computers, smartphones and tablets.

7.1. General recommendations for Internet users

Installing a security solution: A stable security solution is one of the fundamental tools of an Internet user. In addition to virus protection, it should include a firewall, spam filter and real-time protection against threats on the web, and receive regular updates periods.

Install all updates: It is recommended that all other operating systems and installed applications to be fully updated by downloading patches, service packs and updates available. Obsolete programs that is no longer supported by the supplier should be replaced with new versions.

Deleting unused accounts online: online payment services, social networking, online stores, email service providers - Internet users have a wide range of different online accounts. It is worth checking their necessity and where data access is no longer used be deleted for security reasons.

Change passwords: It is recommended regular change of passwords used in online stores accounts, social networks and other portals on the net. Secure passwords consist of a sequence of numbers, special characters, uppercase and lowercase. Caution: avoid common terms as may facilitate the work of hackers.

Saving data: A backup function can save important data, such as pictures or videos from vacation with his family, where the system fails after infection. In addition, the system can save an image of your entire hard disk with all installed programs. Complete security solutions include backup module without the need for dedicated software purchase.

7.2. Recommendations for mobile devices

Securing smartphones and tablets: Mobile devices have the same need for security as computers. It is recommended that they are equipped with comprehensive security applications. These should include reliable protection against malicious applications and ensure devices against the consequences caused by a possible loss.

Applications only from trusted sources: It is recommended that applications be downloaded only from trusted stores like Google Play or from retailers to suppliers and device manufacturers. When this is done in this way should be thoroughly checked permissions requested.

Backup computer: Users should save regularly computer data on smart phones or tablets in order not to risk losing them.

8. CONCLUSION

In conclusion, the best protection against theft of sensitive information is data encryption. Although it sounds complicated, encryption is a complex tool, meant only for big companies [9]. Encrypting information of customers alongside their financial data and other important information, you can ensure that information is protected from attempted theft or accidental losses.

9. REFERENCES

[1] Adams, A. (2005). *Review: Cyber Ethics: Morality and Law in Cyberspace*, International Journal of Law and Information Technology, **13(2)**, 289 - 291;

[2] Laudon, K. C. (1995). *Ethical concepts and information technology*, Communications of the ACM, **38(12)**, 33 - 39;

[3] B2B International, (2014) *Global Corporate IT Security Risks: 2013*, (Accessed in June 2015), http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf

[4] Kaspersky Lab, http://www.kaspersky.ro/business_products (Accessed in May 2016);

[5] Ernst & Young (2016) - *Global Forensic Data Analytics Survey – Shifting into high gear: mitigating risks and demonstrating returns*;

[6] B2B International, (2013). *Security in a multi-device world: the customer's point of view*, (Accessed in May 2015), http://media.kaspersky.com/pdf/Kaspersky_Lab_B2C_Summary_2013_final_EN.pdf

[7] Kaspersky Lab, (2016). *Kaspersky Internet Security – Multi-Device,* http://www.kaspersky.ro/internet-security-multi-device (Accessed in July 2016)

[8] Poneman Institute, (2016). *Infractorii cibernetici vizează informaţiile confidenţiale ale clienţilor agenţiilor mici de marketing,* http://www.agora.ro/stire/infractorii-cibernetici-vizeaza-informatiile-confidentiale-ale-clientilor-agentiilor-mici-de-m#sdendnote1sym (Accessed in August 2016);

[9] European University Institute, (2013), Code of Ethics in Academic Research (2013 Edition), Italy: European University Press. Retrieved from http://www.eui.eu/Documents/ServicesAdmin/DeanOfStudies/CodeofEthicsinAcademicResearch.pdf (Accessed in August 2016)