THE IMPACT OF ECONOMIC COMPANY DATA THEFT

Student, Ramona MARGE[1], PhD, Ştefan IOVAN[2,3]
[1]Oradea University, Mathematics Faculty, ROMANIA, ramona.marge@yahoo.ro
[2]The West University of Timişoara, Computer Science Department, ROMANIA
[3]Railway Informatics SA, Bucharest, ROMANIA, stefan.iovan@infofer.ro

Abstract: *Cyber security remains one of the hot topics in the context of a steady increase in the number of Internet-connected devices, new device classes and new architectures, which are as many potential levers for cyber criminals. At the same time, they are increasingly oriented towards macro attacks at the Internet infrastructure level to maximize their benefits. Companies adopt complex security solutions. To this end, there are platforms that provide a wide range of tools and technologies to enable companies to control and protect all devices on the network. In terms of preventing internal threats, solutions have powerful encryption algorithms that protect important business information, application control tools, device control, web control and mobile device management features to implement IT security policies. The solutions created by specialists provide effective protection against all types of threats on the Internet and help maintain productivity at work with simple web policies that can limit employees' access to social networks, online gaming, or other sites during working hours. The paper aims to present some aspects of computer cyber attacks on data, information, applications, and company systems using mobile devices. The subject is vast and generous, and this paper will only touch on some aspects of cyber security.*

Keywords*: cyber security, data theft, spam, viruses, financial trojans, hackers;*

1. Introduction

The new technologies, the rapid spread of mobile devices, wireless communications and the growth of the user base have opened new gates of opportunity for cybercriminals. Here are some of the most striking aspects that have occurred in recent years [1].

Digital certificates - Signed viruses with stolen digital certificates are not a novelty, but they are a major trend in the industry. We expect the volume of malicious software signed with illegally acquired digital certificates to grow a lot, and the trend will continue, especially in the gray area of software, such as adware and spyware.

Internet on increasingly diverse devices - By 2015, the number of Internet-connected terminals worldwide reached 25 billion, and by 2020 it will double. These include vital function monitoring devices, medical devices, onboard car computers, emergency signaling devices, household appliances. Each with their own security settings, they will become the main target of computer criminals.

Mobile phones and tablets - The Android operating system currently has about 70% of the mobile operating system market, which makes it very relevant to computer scams. If we take into account that mobile terminals are also means of payment (via sms to over-charge numbers or new payments through *Near Field Communication* – NFC), hackers will increasingly focus on creating viruses for Android. Increasingly frequent use of personal phones at work and vice versa will allow hackers to better target companies and individual users.

Email spam is decreasing, but advertisments adapted to social networks are increasing. Spam has been used since the beginning of electronic communications and has gained market share in the botnet era. While the amount of spam will continue to be high, scammers will focus

more on social networks where they can better target victims. Unmanned spam attacks will continue to be used and will contain malicious documents that will install botnet viruses on your computer.
The old technologies will still be popular. Suspension of Windows XP support (end of April 2014) allowed hackers to attack operating system users once it was not maintained by updates. In particular, those in the business environment still using Windows XP will be affected.
Smart clothing accessories, such as medical bracelets to monitor vital signs connected to the Internet, are becoming more and more popular all over the world. Reduced dimensions and focus on battery life leave little room for security, which could bring them to the attention of hackers in the near future, though not necessarily now.
Medical devices - Just like intelligent clothing accessories, medical devices are becoming more and more interconnected. Wireless communications abilities allow doctors to monitor patient health and device performance, but can also allow unauthorized entities to manipulate equipment and even cause the death of the patients.
Social networks - With more than two and a half billion active users on Facebook, social networks are used by hackers to gather knowingly distributed information by users, which they can then use in targeted spear-phishing attacks or to distribute computer threats.
More and more dangerous viruses - Botnets (or viruses that turn the user's computer into an attack tool) are still the backbone of any criminal operation, from DDoS attacks to spamming or the accumulation of Bitcoins on the victim's account.
Scammers will focus on exploiting outdated software to turn victim computers into components of an attack network [2]. Most of the big botnets will use peer-to-peer communication models to keep them from being blocked, while the smaller ones will use social networks as a back-up communication mechanism with command and control servers.
The volume of viruses exceeded 250 million copies in 2014 due to *polymorphism viruses*, a feature present in almost all major software packages on the black market.

2. The impact of the human factor in it security

Most companies around the world understand the importance of preventive IT security measures and implement them. This is because 87% of Eastern European companies have experienced an internal security incident that has led to loss of information, according to the study [3]. According to the study [3], the three most common types of internal threats are: vulnerabilities or defects in existing software, security breaches caused by a human error, and the loss or theft of mobile devices.
To minimize internal security risks, 57% of the surveyed organizations have network structures that separate "*mission-critical"* networks from other networks, and 51% of companies have implemented different levels of access to IT systems. However, many companies consider that existing measures are insufficient and are implementing more and more new security solutions that implement security policies and provide additional protection against leakage of information.
For example, less than half of the surveyed companies use application control, device control, or anti-malware for mobile devices. An even smaller number of organizations have implemented a *Mobile Device Management* (28%) solution or mobile device encryption solutions (36%).
Another problem is that employees do not always follow the company's existing security policies, and moreover, less than half of the firms (32%) have set clear disciplinary measures

and disciplines for situations where security policies are violated. Meanwhile, less than half (only 33%) of surveyed companies believe that security policies are valued by company staff. In addition, the results of the study [3] reveal that small and medium-sized businesses around the world have an even lower level of use of corporate security solutions.
Solutions also offer business owners the ability to limit file downloads and block access to various applications, protecting the company from malicious software disguised as legitimate programs.

2.1. "Financial" trojans landscape

The number of "financial" trojans, created with the aim of gathering as much financial data as users, has increased more than three times, namely by 337% in 2014 compared to 2013. Also, the number of computers that would be could be infected during this period exceeds 500,000 each month, according to an earlier report [4].
Institutions from over 100 countries, including 1,400 financial institutions, have been attacked through this type of financial trojans. The top 15 banks were attacked using at least 50% of existing financial trojans. The institutions targeted by the majority of the attacks are from the US, and in their case, 71.5% of all the trojans analyzed were identified. Moreover, there is a continuing expansion of the attacks on institutions in the Middle East, Africa and Asia.
For the report [4], more than a thousand configuration files from eight online banking trojans were analyzed. Among the clonclusions, it has been determined that attack techniques range from redirecting browser pages to other sites, to complex code "*injections*" that allow automated transactions in the background without being perceived by users.
The data show that most of these infections – over one million – were recorded in the United States. The following places were Japan – 206,000, Great Britain – 178,000 and Canada – 118,000. Also, as the Bitcoin value grows, there is also growing interest in creating special malware, such as *ramsonware*. The most used trojans in the past years were the *Zbot* + *Gameover*, which compromised over two million computers, *Cridex* – 125,000 computers, and *Shylock* – 33,000, only in the first nine months.
Among the most important findings of the study [4], we mention the growing expansion of attackers' operations in new markets. Are becoming increasingly Interesting the countries popular for the large number of wealthy citizens, such as Saudi Arabia, and also the money-transfer services where most of the high-value transactions such as ACH in the US and, more recently, SEPA in Europe.

2.2. Financial data is the target of spam in Romania

The proportion of spam in e-mail traffic continues to decline – in recent years, the unsolicited message share has fallen by 10.7 percentage points. Thus, it appears that advertisers are increasingly focusing on other types of legitimate online advertising that are now available and which have a higher response rate at lower costs than spam. Experts have summarized the spam activity of recent years as follows:

- The proportion of spam in the email flow was 69.6%, 2.5 percentage points lower than the previous year;
- The proportion of spam sent via computers and servers in Romania was 1.32%, with Romania ranked 13th worldwide;
- The percentage of emails with malware-related attachments was 3.2% - 0.2 percentage points lower than the previous year;
- 32.1% of phishing attacks targeted social networks;

- The main sources of spam were China (23%) and the United States (18%).

Spam commercially promotional messages are gradually being replaced with those of cybercriminals such as spam that promotes illegal products or pornography. A typical example is e-mail in the "*Travel and tourism*" category, used in 5-10% of total spam traffic. Currently, such advertisments are rare, but experts have seen numerous malware emails that actively exploit themes such as holiday and leisure offers.

Typically, IT security experts recommend users update their antivirus solutions periodically, and cybercriminals have tried to take advantage of non-upgrading antivirus solutions.

In emails that seem to be sent by well-known antivirus vendors such as Kaspersky Lab, McAfee, ESET, Symantec, etc., they asked users to update their systems as soon as possible using the attached file. But the attachment contained a Trojan from the *ZeuS/Zbot* family, designed to steal important user data, especially financial information.

For the third consecutive year, the most common e-mail malware were programs designed to steal confidential information, typically login data and passwords for online banking systems.

But phishing attacks are now moving from bank accounts to social networks and e-mail. This can be partly explained by the fact that emails nowadays often provide access to a wealth of information, including accounts on social networks, instant messaging services, cloud storage, and sometimes even and credit card details.

In an attempt to reach as many users as possible, but aware of the presence of spam filters that block unwanted messages, advertisers use various tricks. Part of mass mail is sent to subscribers who have agreed to receive promotional messages, and another is sent to addresses taken from huge purchased databases – to people who have not given their consent to receive such messages.

If e-mails are blocked by spam filters, the advertisers contact their security vendor and try to demonstrate that their messages are legitimate, showing the site where users sign up and where they can unsubscribe at any time. This situation represents a new challenge for the anti-spam industry and leads to the development of new technologies that analyze the reputation of the sender.

Asia is responsible for 55.5% of global spam (5.3 percentage points higher than last year), followed by North America by 19% (+ 3.2 points). The share of Eastern Europe has almost doubled since last year, placing the region in the third place with 13.3%. Western Europe remains fourth, despite a 2.4 percentage point decrease from the previous year, while Latin America ranks fifth, down one third from last year's figure.

3. Safety of online transactions

The evolution of online banking has triggered a new type of cyber crime – the theft of bank information. Criminals are continually developing new ways to bypass financial data protection systems. From the analysis of online banking systems, experts have discovered how malware programs can steal users' money and how they can protect themselves against attacks.

Banking trojans are the most dangerous type of specialized malware. Once installed on the victim's computer, a Trojan automatically collects all payment information and sometimes even finances on behalf of the victim. Offenders use multiple-purpose bank trojans that can affect customers of different banks and payment systems, as well as trojans scheduled to attack customers of a specific bank.

Offenders can send trojans through phishing emails to help convince a user to access a link or open an attached malware document. For mass distribution of bank trojans, they use Windows

vulnerabilities and other popular applications.
Once they get into the system, these exploits launch a Trojan on the infected computer. To attack more effectively, offenders use exploit packages tailored for various vulnerabilities. Once they have entered an infected computer, the trojans use the following techniques:

- *Keylogger is intercepted*. Trojans detect the keys used by the user, helping criminals steal online banking user account data.
- *Screenshots* while displaying the completed financial information form.
- *Recording of virtual keyboard*, providing criminals with details of the symbols typed on this keyboard.
- *Changing host files*, which redirects users to false sites, even if the site address is entered manually.
- *Injection in browser operations* allows trojans' control over browser connection to server. The criminals can get the account data that the user fills in on the bank's website and modify the online banking system's opening page by adding additional forms (*webInject*) that request the credit card number, the name of the holder, the expiration period, the CVV code, password, etc.

In addition, bank trojans can go beyond additional security levels, such as two-step password-only authentication (*TAN*s). One of the techniques used by the *ZeuS* Trojan works as follows: as soon as the victim accesses an online banking system and enters the unique password, the malware displays a false notification that conveys the message that the existing TAN list is invalid, inviting the user to get a new password list.
To do this, the victim has to enter all the available TANs in the forms created by ZeuS by the WebInject method for "*additional lock*". As a result, offenders are able to get all the victim's codes, which they can immediately use to transfer money to their own accounts. Only in 2012, more than 3.5 million attempts were made to attack 896,000 computers from different countries [5, 6].
Although it seems a problem without solving, there is a solution – as new technologies demonstrate. At this time, financial information is protected by antivirus solutions and specialized technologies such as *Safe Money*, which protect users against bank trojans using antivirus, browser security, and keyboard security, while the authenticity of the payment or system of online banking is checked against its digital certificate and link.

4. Conclusions

About 7% of the advertisements displayed on legitimate websites target users to pages containing viruses, send them fraudulent messages, spam, or phishing messages, according to a Bitdefender study of 70,000 banner advertisments showing approximately 150,000 of web pages. To select advertisments, the research team scanned search engines after 50 terms like free movies, free music, games, torrents, free download, lose weight now, earn money from home, terms that users frequently search for.
The most dangerous advertisments are part of the business category and represent 20.73% of the total. This category covers fictional business websites, websites created by scammers to promote fake product offers at very low prices [7]. Another 20% of the dangerous ads identified on legitimate sites are in the category of those who provide computer or software information and services on the internet, such as false SEO plugins, video converters, or cursors.
More than 12% of fraudulent advertisements refer to online casinos, another 12 percent are advertisements for medical products and services, and 5% of dangerous banners promote

pornography.
We expect scammers to exploit more and more advertisments to deliver malware or mislead them into various games where they lose money. Millions of users around the world are exposed to virus infections, fraudulent messages, or spam. An example of the effects this phenomenon might have is the incident involving the Yahoo! portal in 2014.
In early 2014, Yahoo! visitors were infected simply by accessing the portal because of a malicious banner. This led to a Java exploit that loaded a vulnerability through which the user could be infected with very dangerous viruses like Zeus or Dorkbot. Also, in September 2009, New York Times readers were directed through an infected advertisement to a site hosting dangerous software.

These examples show that malicious advertising has become one of the most dangerous threats, because it can spread on a large number of legitimate sites and can thus reach a large number of users. In addition, some of the banners allow scams to infect users without actually clicking on them.

References

[1] IOVAN, Şt. and IOVAN, A.-A. (2016) *FROM CYBER THREATS to CYBER-CRIME*, Bucureşti: Editura Universitară, *Journal of Information Systems & Operations Management*, (***JISOM***), Vol. **10**, No. **2**, ISSN: 1843-4711, pg. 425 - 434;
[2] IOVAN, St. and MARGE, R. (2017) *Some Legal Aspects on Cybercrime*, Targu Jiu: "Academica Brancusi" Publisher, *Annals of the "Constantin Brancusi" University, Engineering Series*, Issue **3**/2017, (***CONFERENG 2017***), ISSN: 1842 – 4856, pag. 181 – 186;
[3] B2B International, *Global Corporate IT Security Risks 2013*, https://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf , (accessed in may 2017);
[4] Symantec, *The State of Financial Trojans 2013*, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/The_State_of_Financial_Trojans_2013, (accessed in october 2016);
[5] IVANUS, Cr. and IOVAN, St. (2017) *Cybercrime in the European Union*, Targu Jiu: "Academica Brancusi" Publisher, *Annals of the "Constantin Brancusi" University, Engineering Series*, Issue **3**/2017, (***CONFERENG 2017***), ISSN: 1842 – 4856, pag. 187 – 192;
[6] IOVAN, St. (2015) *Big Data Security Problems*, Proc. of 16th European Conference (***E_COMM_LINE 2015***), Bucuresti, Romania, ISSN: 2392-7240, ISSN-L: 2066-6829;
[7] IVANUS, Cr. and IOVAN, St. (2015) *Internet – The Foundation for the Future Societies Permanently Connected*, Proc. of 16th European Conference (***E_COMM_LINE 2015***), Bucuresti, Romania, ISSN: 2392-7240, ISSN-L: 2066-6829;