DOI: 10.26411/83-1734-2015-1-41-6-19

Effective Protection of Information Systems and Networks Against Attacks in the Era of Globalization

Katarzyna Witczyńska
Wroclaw University, Poland

In the era of globalization, more and more threats to the IT systems of many global companies will be observed. More and more attacks are effective and the losses caused by intrusions are systematically growing. The problem of ensuring the security of networks and computer systems is one of the most important issues of modern computer science. Today, more research is being done around the world to ensure the security of operating systems and applications.

Keywords: globalization, information systems, security systems, international trade, internationalization

1. INTRODUCTION

Nowadays, the number of threats for IT systems is constantly growing. More and more attacks are effective, and the losses caused by intrusions are systematically growing. The problem of ensuring the security of networks and computer systems is one of the most important issues of modern computer science. In scientific centres around the world, numerous studies are carried out to ensure the security of operating systems and application programs. The aim of the work is to provide theoretical and practical knowledge related to threats, security methods and the latest trends in effective protection of networks and information systems against attacks.

It is not possible to achieve complete security of IT systems. This is related to the problem that is unsolvable in the field of computer science, which is the occurrence of errors in computer programs and the unpredictable ability of intruders to use some fragments of their code. In practice, it is not possible to create a complex computer program, including an operating system that would be completely free of errors. Every working computer program has fragments of code, which under certain conditions may generate an error, which can sometimes lead to access to computer resources by an intruder [9].

The security of data management in computer networks is one of the most important tasks of modern information and communications technology. Information security means protection of information and information systems against unauthorized access, use, disclosure, disruption, modification or destruction. In the article it will be presented the basic types of malware, a broad description of network security and the latest trends in effective protection against attacks using different types of antivirus programs.

Cybercrime in 2019 is a threat worth $ 2.1 trillion. Companies must constantly take new actions, use the latest trends to effectively protect networks and information systems from attacks. The World Economic Forum (WEF) claims that much of cybercrime is undetected, especially industrial espionage, where it is difficult to see access to confidential documents and data. Cybercrime is developing the market for IT network security products and services, whose share in the IT market is expected to increase from USD 75 billion in 2015 to USD 175 billion by 2020 [13].

2. TYPES OF MALICIOUS SOFTWARE

Malware is a term referring to various hostile programs, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware and other malicious programs. They can take the form of executable code, scripts, active content and other software. Malicious software is defined by malicious intent, acting against the requirements of a computer user - and therefore does not include software that causes unintentional damage due to some shortcomings. The operating system according to scientific definitions is an organized set of programs (systems) that act as an intermediary between the equipment and the user, provide the user with means to facilitate the design, coding, running and operation of data processing programs [6]. The operating system is the largest computer program, the source code of the Microsoft operating system - Windows XP has 40 million rows [5]. This value shows how great potential malware authors are, looking for vulnerabilities and how to bypass embedded security.

The security of information sent over the Internet is mainly about ensuring the security of websites, while hacking into computer systems where websites are run is a common phenomenon. The targets of attacks on operating systems of this type are increasingly being carried out. Sometimes websites that have been successfully attacked are used to share malicious programs (e.g. Trojan horses). Visiting such a website may result in the installation of software on unsecured computers that may be used, for example, to steal passwords of access to bank websites [32].

Malicious software should be applied directly to the user's computer. The effects of their operation are system damage, data destruction, as well as disabling access to networks, systems or services. Malicious software can also steal data or personal information from the user's disk and send it automatically to cyber criminals. They usually have the ability to replicate themselves and spread to other hosts attached to the network. It happens that these techniques will be used in conjunction with social engineering to "cover up" the careless user (it is known that this will trigger the attack). Viruses, worms and Trojans are just examples of malicious software.

Virus means a computer program usually hidden in another seemingly innocuous program that produces copies and inserts them into other programs or files that usually perform malicious activity (e.g. data destruction). The principle of operation is also based on spreading through the modification of other programs or files. It is not possible to "call" the virus itself, it must be intentionally activated. Once activated, it can do nothing but replicate and spread. The simplest virus can be dangerous, because it can quickly use all available computer memory and bring the system to a halt. In the case of more complicated viruses, it can happen that they will delete or damage files. Virus transfer can take place via e-mail attachments, files, messengers, CDs or USB devices. Computer viruses can be characterized as:

- parasitic - use victims for transport
- polymorphic - changing their source code
- batch file viruses - they use files with the .bat extension for transport.

The most popular viruses include: Chernobyl (CIH), Christmas Tree.

Worm - worm resembles a virus, the difference is that it does not have to join an existing computer program. The principle of operation is compared to an independent computer program, but it contains malicious software that repeats itself to spread to other computers. It often uses a computer network to spread, relying on security failures on the target computer to access it. Worms almost always cause at least damage to the network, even if they only consume bandwidth, while viruses almost always damage or modify files on the target computer. There are known examples of worms that have been created and are intended only to spread and do not attempt to change systems. However, the Morris and Mydoom worms have proven that "unloaded" worms can cause significant disruptions by increasing network traffic and other unintended consequences. Network worms create a greater threat than a single virus, because they can "infect" large areas of the Internet. The most popular worms include: Netsky, I Love You, Morris, Melissa, Mydoom.

Trojan Horse called a “computer Trojan” in a computer language/slang is a malicious computer program that misleads users under the cover of a real intention. The term comes from the ancient Greek story of a fraudulent wooden horse that led to the fall of the city of Troy. Trojans are generally disseminated by some form of social engineering, for example in the case where a user is cheated to read masked e-mail attachments (e.g. a routine form to be completed) or by downloading. The Trojan may allow an attacker to gain access to users' personal data, such as banking information, passwords or identity (IP address). Ransomware attacks are often also carried out using a Trojan. Unlike computer viruses and worms, Trojans usually do not try to inject themselves into other files or otherwise propagate themselves. The most known Trojans are: Connect4, Flatley Trojan, Poison Ivy.

Logical bomb - a piece of code deliberately inserted into the software system that will disable the malicious function when certain conditions are met. Software that is inherently malicious, such as viruses and worms, often includes logic bombs that carry out a specific load at a specific time or when another condition is met. This technique can be used by a virus or worm to gain momentum and spread before it is noticed. Some viruses attack host systems on certain dates, e.g. on Friday, April 13 or April on April Fool's Day. Emergency Trojans are often called "time bombs" on specific dates. In October 2005, Mark Russinovich discovered that Sony BMG installed in its music discs a logic bomb that silently and without the consent of the user installed malicious software on their clients' computers. This software monitored and sent music playing habits. The remote access paths opened by the Trojan were unprotected and could be used by other malicious software. About 22 million of CDs [14] came into use.

Exploit - the word comes from the verb: "to use something for your own benefit" is a piece of software, data or a sequence of commands that uses an error or a flaw causing unintentional or unexpected behaviour occurring in computer software or electronic equipment. This behaviour often includes things such as gaining control of a computer system, allowing privilege escalation or a denial of service (DoS or related DDoS) [11].

Keylogger is software designed to steal passwords by registering keys hit on the keyboard, so that the person using the keyboard is not aware that the actions are monitored. Keylogging can also be used to study human-computer interaction. There are numerous methods of keylogging: from hardware and solutions based on software for acoustic analysis. Keylogging can be done without installing the software and can consist in modifying the BIOS firmware (based on the integrated circuit based software) or installing a hardware circuit between the keyboard and the computer that registers keyboard operation [15].

Ransomware called also ransom is a type of malicious software from cryptology that threatens to publish victim data or perpetual blockage of access, unless the ransom is paid. While some simple ransomware can block the system in a way that is not difficult for a person who can reverse, more advanced software uses the cryptoviral enforced technique in which it encrypts the victim's files, which makes them unavailable and require payment of a ransom decrypt them. As part of the acquisition of ransom are used to track digital currencies, such as Ukash and Bitcoin, making it difficult to track and prosecute perpetrators. The ransomware called CryptoLocker was especially profitable, getting about 3 million US dollars before it was liquidated by the authorities, and CryptoWall was estimated by the US Federal Bureau of Investigation (FBI) for 18 million dollars in June 2015 [12].

Rootkit is a collection of computer software, usually malicious, designed to allow access to a computer or areas of its software that would not be allowed (for example to unauthorized users). The term rootkit is a combination of "root" (the traditional name of the privileged account on Unix operating systems) and the word "kit" (which refers to the software components that implement this tool). The term "rootkit" has negative associations due to the connection with malware. It is a program that allows you to enter a computer system by hiding malicious files and processes that have power over the system. Discovering a program on a damaged computer is difficult because it is able to check the work of specialized tools that are used to detect. The most popular include: Hacker Defender, Sony Rootkit CD. Literature describes cases of commercial use when rootkits were installed deliberately by the owner of the system or a person authorized by the owner, e.g. to monitor employees [7]**.**

Spyware its purpose is to collect information about the user (websites visited by the user and other sensitive data are visible). Spyware is usually classified into four types: adware, system monitors, cookie tracking and Trojans. Examples of other known types include digital rights management functions that "call for home", keyloggers, rootkits. The most known spyware are: Gator, Cydoor, Save Now.

Stealware is a type of malicious software that transfers money or data to a third party. The stealware software uses an HTTP cookie to redirect normal website earnings to direct users to another site. This software is used to steal the unconscious user - this results from the tracing of the activity [3]. The installation of the software takes place without the knowledge and confirmation of the user by means of adequately prepared viruses, worms or websites using errors and gaps in web browsers. The stealware program when registering the online payment changes the account number to which funds will be paid.

3. TYPES OF ANTIVIRUS PROGRAMS

Analysing and evaluating modern practices in the subject of securing computer systems, it should be stated that the possibility for the intruder to gain access to the operating system cannot be eliminated. However, reducing risk in information technology is not only about eliminating unwanted events, but also reducing the negative effects of such an event. For this reason, the protection of computer systems, in addition to preventive measures, also includes detecting and responding to threats [2].

Antivirus software (called the AV shortcut) is computer software used to prevent, detect and remove malicious programs. Antivirus software was originally developed to detect and remove computer viruses, hence its name. However, with the proliferation of other types of malicious software, antivirus software began to provide protection against other computer threats. Modern anti-virus software can protect against: malicious browser objects, ransomware, key loggers, backdoors, rootkits, Trojans, worms, scams, adware and spyware. Some products also include protection against other computer threats, such as infected or malicious URLs, spam, scams, phishing attacks, attacks on online banking data and DDoS attacks.

Scanner is used to find bytes in the data string. Such a device is better when the virus has a characteristic inscription or sequence of bytes. Thanks to polymorphic viruses, the importance of scanners has decreased, but it is still an important way to deal with viruses. Polymorphic viruses are virtually impossible to detect because their samples are not the same. Very often, different virus samples do not have a common part. Polymorphism is possible thanks to the virus coding. In a later phase it is possible to use the scanner [1].

Monitor - resident monitor is antivirus software used in the operating system - so-called resident program - TSR (Terminate and Stay Resident) or SYS type driver. It works by monitoring the DOS function and the BIOS, which makes it possible to discern the disk references made with these systems. The effectiveness of the monitor results from the fact that it has control over the system or the activity of the virus and how much it enters the operating system.

Vaccine - disinfector is anti-virus software. It counteracts specific infections. After identifying the virus and analysing the code, you can search for the characteristics that allow you to prepare the right vaccine.

Self-verifying programs are used to verify that the program has not been changed by the virus. The analysis is possible by attaching to the indicated program file. The attached code is added to the file using the same mechanism as the virus and allows self-verification. Its purpose is to detect whether a given program has changed. This is done by counting checksums for the requested file or files. The calculated check sums are stored in separate files created after the first start of the program. In case the files were present before, the antivirus program should download the data contained in them to compare the currently counted sum with the sum from the previous file.

Checksum counting program - integrity checker is a system that calculates files on disk for the first time and then uses this data to analyse with the current checksum and detect the presence of the virus.

On-line antivirus scanners are a full-featured tool that allows you to remove detected threats from any computer using a web browser without having to install an antivirus program on your computer. Antivirus vendors maintain sites with free online scans across the entire computer, only in critical areas, local drives, folders or files. Periodic online scanning is a good idea for those that run antivirus applications on their computers, because these applications are often slow to catch threats. One of the first things that malware does during an attack is to disable any existing antivirus programs, and sometimes the only way to learn about an attack is to go online resources that are not installed on the infected computer [4].

4. SUMMARY

In the great business IT market, influence of globalization is difficult to overstate. It has altered main strategy, recruitment process and infrastructure. It is also providing new breakthrough management styles from the high level of the IT Companies. During the TIF – The Corporate IT Forum, organization with representation in IT management of Financial Times Stock Exchange London - 500 companies, globalisation has become a hot topic [17]

The insufficient number of IT specialists qualified cyber security specialists on the market is growing and the expected gap in human resources will reach 1.8 million jobs by 2022. Lack of resources and skills of IT employees prompts many companies to start recruitment wires in advance. A recent ISACA - Information Systems Audit and Control Association published report showed that 55% of organizations stated that recruitment for a position related to data protection and protection against cyberattacks should take at least three months to find the right employee. While 32% say recruitment lasts six months or more. However, 27% of American companies claim that they cannot find the right person at all to fill a position related to protection against cybercrime [16].

BIBLIOGRAPHY

[1] Błaszczyk A., *Wirusy. Pisanie wirusów i antywirusów, Read Me*, Warszawa, 1998.

[2] Cavusoglu H., Mishra B., Raghunathan, S., *The value of intrusion detection systems in information technology security architecture, Information Systems Research*, USA, 2005, pp. 28-46.

[3] Erbschloe M., *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code, Butterworth-Heinemann,* USA, 2004, p. 28.

[4] Krebs B., Online Anti-Virus Scans: *A Free Second Opinion*, Washington Post, USA, 2007.

[5] Maraia V., T*he Build Master: Microsoft's Software Configuration Management Best Practices*, Addison-Wesley, USA, 2006.

[6] Shaw A.C., *Projektowanie logiczne systemów operacyjnych*, WNT, Warszawa, 1980.

[7] Vieler R., Professional Rootkits, John Wiley & Sons, USA, 2007 p. 244.

[8] Wróbel M., *Metody zapewniania bezpieczeństwa systemów operacyjnych* - Rozprawa Doktorska, Politechnika Gdańska Wydział Elektroniki, Telekomunikacji i Informatyki, Gdańsk, 2010.

[9] Yegneswaran V., Barford P., Ullrich J., *Internet intrusions: global characteristics and prevalence, Proceedings of the 2003 ACM SIGMETRICS international conference on Measurement and modeling of computer systems*, ACM, New York, 2003.

[10] Yung M., Young, A., *Cryptovirology: extortion-based security threats and countermeasures*, IEEE Symposium on Security and Privacy, USA, 1996, pp. 129–140.

INTERNET SOURCES:

[11] Astechnica, https://arstechnica.com/information-technology/2015/06/fbi-says-crypto-ransomware-has-raked-in-18-million-for-cybercriminals/

[12] Forbes, https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#48b2c0423a91

[13] https://www.networkworld.com/article/2998251/malware-cybercrime/sony-bmg-rootkit-scandal-10-years-later.html

[14] Pctools, http://www.pctools.com/security-news/what-is-a-keylogger/

[15] Techrepublic, http://www.techrepublic.com/article/4-tips-to-help-your-business-recruit-and-keep-cybersecurity-pros/

[16] XComputerweekly, http://www.computerweekly.com/feature/Globalisation-IT-management-strategies

Date submitted: 7-02-2018
Date accepted for publishing: 2019-04-30

Katarzyna Witczyńska
Wroclaw University, Poland
katarzyna.witczynska@uwr.edu.pl