SOURCES OF THREATS AND THREATS IN THE CYBER SECURITY

JAN SVOBODA, LUDEK LUKAS

Abstract: *The article presents a brief analysis of selected threats to their sources. The introduction presents the difference between the source of the threat, the threat and the risk. In the next chapter, attention is paid to the most commonly occurring threats in cyberspace and the following are specific sources of threats responsible for individual threats. The actual process of spreading specific threats in cyberspace, the relationship between the threat and the reference object and the difference in targeting the threats towards the reference objects are already listed in the last chapter. Predictions of future threats and necessary protection tools are listed in the final chapter.*

Key words: *Cyberspace, Source of the Threat, Reference Object, Targeted, Omnidirectional*

Authors´ data: Svoboda, J[an]; **Lukas**, L[udek], Tomas Bata University in Zlín nám. T. G. Masaryka 5555, 76001 Zlín, CZ, j3svoboda@utb.cz, necesal@fai.utb.cz

This Publication has to be referred as: Svoboda, J[an] & Lukas, L[udek] (2019). Sources of Threats and Threats in the Cyber Security, Chapter 27 in DAAAM International Scientific Book 2019, pp.321-330, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-24-2, ISSN 1726-9687, Vienna, Austria
DOI: 10.2507/daaam.scibook.2019.27

1. Introduction

Cyber security is a relatively new field of security, and so cyber security is associated with progressive developments and a wide range of threat sources. The risks of cyber threats are changing in the context of globalization, the level of security environment and security education of administrators and users operating in the information and communication environment. The correlation between sources of threats and threats has changed since the emergence of cyber security, when the main source of the threat was mostly a person, organized group of people, or a society with a certain interest, whereas the threat has changed according to variable conditions depending on the number of organizational, software and hardware gaps in the communication and information environment. However, the source of the threat is not just the attacking entity, but a source of threat may also be the lack of a security tool, user and administrator behaviour and finally, some software or hardware component of the device inside the communication and information environment. The threat analysis over time corresponding to the development of cybernetics in general expresses current trends in cyber security and partially predicts the occurrence and interrelationship between threat sources and threats referred to in this article.

2. Source of threat, threat and risk

The source of the threat is the entity carrying the effects of the threat. It can be a living, inanimate, tangible or intangible object and this object can threaten our reference object (protected interest).

The threat is most often called as a phenomenon and this phenomenon affects a reference object and can damage it. The threat can be specified as an activity or event which causes damage or complete destroys the reference object. The threat can more generally be characterized as a property of the source of the threat which can cause any damage.

Risk is the probability that there will be a threat. Risk is therefore not only probability that there will be a threat but so there will be also some probability of damage too.

3. Sources of threats, threats and risks in cyber security

Basic security breaches are described in this chapter, own characteristics, historical development and present occurrence and the probability occurrence of these disturbances in the future. Acquired data are taken from CSIRT Czech Republic, and the office incorporates relevant data and provides statistics to the public. Due to the fact, many of the security breaches in cyberspace are not subjected to authorities, so it is probability that the finite numbers of security breaches are higher.

a. Social Engineering (Sociotechnics)

Social engineering is different from the security breaches listed below in the form of an attack. The attack is aimed at obtaining private or classified information, and it does not have to be conducted directly in cyberspace. Specifically, it is the ability of an attacker to manipulate, persuade or influence an authorized person and so forces the person to act to provide the private information needed to the cyber-attack. The most common threats to social engineering include obtaining the necessary information by collecting and analysing freely available data or providing the necessary information to an "illegal" person with a changed identity or through a targeted professional psychological attack.

The main tools of social engineering include:

- fraudulent email or fake website phone call,
- face-to-face attack,
- garbage analysis,
- search the web, social networks, and other online publicly available information,
- delivery of advertising or other materials on CD, DVD or other storage medium,
- freely accessible or forgotten storage media,
- try online service offerings,
- supply or find equipment, using a different identity.

The source of the threat with the use of social engineering can generally be identified as an attacker and thus an individual or organized group of persons. The source of the threat is therefore the person or persons.

Historically, social engineering has occurred since the late nineteenth century, when the main idea of social engineering was the need to motivate many people to a certain goal Then social engineering flourished as an instrument of individual people but also big corporations and powers. Social engineering is currently being used as part or support of a phishing attack in cyber security or as a tool to retrieve access data. Social engineering is still a major threat that is still growing as a tool to retrieve access data.

b. Botnet

A botnet is a “large computer network” in a public communications and information environment, and its goal is to perform illegal activities using the high computing power available from each botnet computer. The most common botnet activities are ransomware, phishing, spam, data theft, DDoS, etc. Violation of botnet security is a breach of the security of a computer or computer network. The main threats are loss of computing power, loss of privacy and loss of control over the device itself.

The main botnet tools include:

- main management element (establishment of basic infrastructure),

- malware (spreading malicious software to control a device),
- device management, as a rule “client-server” or per peer.

The source of the threat using botnet is generally an attacker that means a person or an organized group of people. Furthermore, they can be a source of threat to devices already included in the botnet. The source of the threat is therefore the person, person, or hardware on the network.

Botnet occurs since 2000, when the first botnet network called EarthLink Spammer was created. This first botnet was used to distribute spam and phishing. Next botnet and the first peer to peer botnet was created in 2007, when some networks operate to the present day. Within the recorded occurrence of CSIRT Czech Republic since 2008, the botnet attack rate to selected information systems has an average of 20.5 cases per year. The malware development trend was highest in 2016.

c. Malware

Malware is an application or software which can usually be covertly installed on a device. In most cases, the user has no idea of the occurrence of malware on their device. The term malware represents a variety of malicious programs and very often infects devices in multiple ways. The purpose of malware is to break the computer's security, install malicious software, and then analyse the environment with the opportunity to expand further. The most common threats to malware are the loss of control over the device, the loss of privacy when using the device, the loss of private and classified information, and last but not least the reduction in computing power or even the functionality of the device.

The main types of malware include:

- Adware (installation of junk advertising software)
- Spyware (private device monitoring)
- Virus (software which connects to an authorized program and then causes various damage to HW and SW and is able to distribute itself)
- Worm (autonomous software which does damage to HW and SW)
- Trojan (software which contains hidden features that threaten the device is not able to propagate without the user's help)
- Backdoor (software which contains hidden functions and opens computer communication ports)
- Rootkits (software which allows masking the presence of malicious software on a device)
- Keylogger (software steals login and password)
- Ransomware (Data loss due to encryption)

The source of the threat using malware is generally devices already included in the botnet. The source of the threat is therefore the hardware or software on the network.

Malware occurs since 1986. Within the recorded occurrence of CSIRT Czech Republic since 2008, the botnet attack rate to selected information systems has an average of 94 cases per year. The malware development trend was highest in 2014 and 2016.

d. Ransomware

Ransomware is software known as blackmail software. The blackmail software is intended to block access users to the device, or his private or classified information for a certain period of time or until the ransom is paid. The original type of Ransomware was a program which blocked users' account. The second generation of ransomware is software that does not block access to the user's computer account but locks and encrypts the user's private and confidential data. Ransomware uses strong encryption algorithms to lock and carefully selects encrypted data, so that the attack targets the most important places in the device system. The goal of ransomware is primarily to earn funds in various currencies. The main threat of ransomware is the loss of important data and data availability is not guaranteed after the requested amount has been paid.

The source of the threat using ransomware is generally devices already included in the botnet or infected device. The source of the threat is therefore the hardware or software.

Historically, ransomware has occurred since 1989, when the first blackmail software was a trojan called AIDS. A massive expansion of ransomware is associated with 2005. Already well known was the Police virus and then Cryptolocker. The threat of ransomware represents the highest threat to ordinary communication and information devices in the present. In the critical infrastructure and CSIRT data, the Czech Republic did not attack cybernetic critical infrastructure ransomware in the Czech Republic.

e. Spam

Spam can generally be described as unsolicited mail, which is sent to the device through a communication environment to platforms such as email client, Skype, Messenger, but also featured on various web applications on discussion forums and other social networks. The goal of spam is sent unsolicited messages, such as spreading advertising, sending malware, spreading fraudulent forms, offers, and ads as social engineering tools. The main threats are filling the mailbox with junk mail, visiting a fraudulent Web site, infecting your device with malware, losing control of your device, losing device performance, enlisting your device on a botnet, or losing private or secret data. Other threats are the loss of funds, damage to health, but also death in the case of buying fraudulent medicines, etc.

The main types of spam include:

Phishing (behaviour to obtain passwords, pins, etc.)
Malware (see chapter above)
Scam (for example: you've inherited money from an American related)
Hoax (chain messages)
Fraudulent offers
Donor ship

The source of the threat using spam is generally devices already included in the botnet or infected device. The source of the threat is therefore the hardware or software. Historically, spam has occurred since the late 19th century, when mass telegram messages began to be sent. In the communication and information environment, spam began to spread in 1978 and most often it was a mass presentation of products of large companies or offers of quick getting rich in offered investments.

f. Phishing, Pharming, Spear Phishing

Phishing is an illegal method in cyberspace using social engineering methods. The goal is to gain access to the user bank accounts or other monetary accounts, as well as a method of obtaining users' personal data. Phishing uses spam to send it to "serious" messages in bulk, which are given links at first glance to serious websites and applications. These pages are only imitations of the originals and are intended to create a sense of security and then the user reveals the information to the attackers. The aim of phishing is to steal victims' funds or personal data. Threats include loss of identity, loss of funds, and existential problems, but even in the case of malware installation, loss of control over your device, loss of your own private data, or enlistment in a botnet.

Pharming is an advanced version of phishing which aims to raise funds, install malware, or personal data. Pharming is an attack on the DNS server of an internet provider, so the user does not know that it is a fake website when visiting his online bank.

Spear Phishing is a targeted phishing attack. The attack is led very often by an organized group and focused on a specific goal. The goal of Spear Phishing is to establish contact with a person within the organization and use that person to access the internal network, install malware, or obtain private or classified data.

The source of the threat using phishing is generally an attacker that means a person or an organized group of people. Furthermore, they can be a source of threat to devices already included in the botnet. The source of the threat is therefore the person, person, or hardware on the network.

Phishing has appeared since 1987, but phishing started to spread around the world only in 2003 and in the Czech Republic in 2006.

g. Hacking

Hacking is a method of knowledgeable person or group of people whose goal is to break computer network security, search for passwords and user account names and obtain private and classified information and other activities.

The objectives of hackers are to detect weaknesses in computer systems, gain financial or information benefits etc. The level of a hacker depends on his or her expertise, experience, and assignment to a group. The main threats to hacking interest are the loss of private data, loss of profit or directly of funds, loss of availability of services, reputation, as well as loss of classified information, information benefits, etc.

The main methods of hacking include:

- Social engineering
- Breaking passwords
- Port scanning
- Using malware to infiltrate a computer system
- Phishing
- Cross Site Script
- Eavesdropping of communication

The source of the threat of hacking is generally identified as an attacker and thus an individual or organized group of persons. The source of the threat is therefore the person or persons.

Historically, hacking has occurred since the 1960s. Originally, hacking was characterized as a way of illegally using commercially available paid services by breaking system security (hardware). In the 1990s, hacking was fully developed into a cyber environment and became a serious cyber security problem.

h. Cracking

Cracking is an illegal activity which aims to break the security of programs and operating systems with a view to their free use in violation of the license agreement. Reasons for cracking are using a foreign program or operating system for your own use, or breaking the security system, and providing a stolen program for public and so providing “clients” with a free but illegal service. Another reason is to break the security of a program or operating system and then infect it with malware to ensure the rapid and efficient spread of other malware. Two methods are generally used to break the program. The first method is to break the program itself and the second is to get a password or a key to use it for free. The main threat of cracking is material and intellectual property damage to the software owner. If a user is using compromised software, the main threats are the consequences of infecting the computer with malware or another malicious program.

The source of the threat of cracking is generally identified as an attacker and thus an individual or organized group of persons. The source of the threat is therefore the person or persons.

Cracking originated in the 1980s. From the outset, cracking has been characterized as a way of illegally using commonly available paid programs and information systems through security breaches. By the 1990s, cracking was already fully developed into cyber environment and became a serious cyber security problem.

i. Sniffing

Sniffing is a method used to analyse data flowing across a computer network. It's about analysing TCP packets with special software. In general, Sniffing is divided into two categories having two completely different goals. The first “legal” goal is to analyse the network in order to optimize it or to search for unwanted or defective communication. The second "illegal" goal is to analyse communication inside the network to search for user accounts, passwords, and other data that the attacker wants. The main threats to Sniffing are the loss of private or classified data, loss of funds, gaining access to user accounts, loss of "know how" or certain benefits, and other events associated with breaking the security of network communications.

The source of the threat using sniffing is generally an attacker that means a person or an organized group of people. Furthermore, they can be a source of threat to special sniffing software. The source of the threat is therefore the person, person, or sniffing software.

j. DoS, DDoS, DRDoS attacks

The purpose of DoS, DDoS, DRDoS attacks is to overload a server (ideally a service provider) available on the Internet or some large network. The aim of the attack is to disable or overload server communication channels by directing queries, or by requesting answers in such quantities, that the affected server is no longer capable of service and is overloaded. The above attacks are divided according to the source of the attack and the method of attack. The source of the attack can be one device (already easy protection when blocking the IP address), or a group of devices mostly from a botnet (complicated protection). The main threat is unavailability of provided services, which can cause other threats according to the characteristics and purpose of the infected server. If a banking institution server is attacked, the provision of mining services is stopped or restricted and the same can be said of attacking a medical institution, transport services, etc. The main threats, according to the characteristics of the attacked server, are the limitations of the services provided and then the damage arises to the property, the healthy and even the lives of people.

The main methods of DoS attacks include:

- DoS attack: one device overwhelming the affected server many queries.
- DDoS attack: many devices (mostly in a botnet) overwhelming the affected server with many queries.

DRDoS attack: Many devices pretended to be an affected server send many queries to know "large servers" that match the actual and affected server.

The source of the threat using botnet is generally an attacker that means a person or an organized group of people. Furthermore, they can be a source of threat to software in devices already included in the botnet. The source of the threat is therefore the person, person, or software in hardware on the network.

Historically, DoS, DDoS, DRDoS attacks have occurred since 1989. The year 2000 and the attack on Yahoo stands became a milestone of DoS attacks. CSIRT Czech Republic has recorded an average of 22 attacks per year since 2008.

4. Comparison of threats, sources of threats and general courses

It is evident from the previous chapter that the main threats are people, malware, affected workstations, and an automated malicious program in the communication and information environment. Threats from threat sources are loss of privacy, loss of personal, confidential and classified data, loss of funds or cryptocurrency, loss of information and communication system functionality, loss of availability of services, damage and destruction of hardware resources as well as damage to health or life.

The basic differences are in the effect of threat sources. First, it's about threat targeting, first a targeted threat or a device-specific attack, on the contrary, the second possibility is spreading in all possible directions from the source of the threat and it depends only on the resilience of the reference object, whether injury occurs.

Effects of threat sources in Cyberspace:

- Targeted
- Omnidirectional

The difference in exposure to threats is linked to the status and jurisdiction of the reference object in the network. Omnidirectional threats mostly affect communication and information devices of ordinary people or users, corporate threats or corporate devices are affected by targeted threats.

Home computers - omnidirectional threat
Corporate computers - targeted threats

Another difference in the effect of threat sources is the interaction between the source of the threat and the reference object. The omnidirectional, and therefore untargeted, attack needs a reference object interaction. The interaction of the reference object is necessary for a successful injury. On the contrary, the outcome of most targeted attacks is not affected by the interaction between the attacker and the victim.

Home computers - mostly user interaction and threat required
Corporate computers - latent threat

Given the evolution of threat sources in the communication and information environment, the most common source of threat is an automated malicious source program. Another is the source of the threat as an infected device, software error of the installed program, hardware error, and up to the tail of the number of sources of threat is already a specific human activity.

Currently, human activity is only an initiator and the subsequent activities, spreading, infecting, undesirable encryption, etc. are done completely automated.

5. Conclusion

In the second half of the twentieth century the development of the communication and information environment led to the immediate emergence and development of sources of new types of threats. Originally, the source of the threat was a human (hacker, or cracker), so the current source of threat is a malicious program (several months to years old) and created on the other side of the globe. This software is fully automated to be able to cause maximum harm to the maximum number of users in the communication and information environment.

The targeting of the threat source has also evolved. Historically concretized and targeted attacks have not ended, but these attacks absolutely overcame the omnidirectional massive global multi-language attacks which cause enormous damage in sum in the number of attacks.

From the above, future threats will be more automated and more sophisticated. It can be assumed that protection against modern threats will require a lot of investment. Investments will be needed in the development of security tools, as well as equipment for rapid system recovery, backup and control of network access, but between devices in internal closed computer networks too.

6. References

Lukáš, L. (2017). Teorie bezpečnosti I., Radim Bačuvčík - VeRBuM,. ISBN 978-80-87500-89-7, Zlín – Czech Republic

Kolouch, J. (2016), Cybercrime, CZ.NIC, z. s. p. o., ISBN 978-80-88168-18-8, Prague – Czech Republic

Lukáš L. and team. (2013), Bezpečnostní technologie, systémy a management, VeRBuM, 2013, Zlín – Czech Republic

Kolouch, J.; Bašta P. and team (2019), CyberSecurity, CZ.NIC, z. s. p. o., ISBN 978-80-88168-34-8, Prague – Czech Republic

https://www.lupa.cz/clanky/historie-a-vyvoj-ransomwaru-vsechno-to-zacalo-s-aids, Lupa.cz, Server o českém Internetu, Historie a vývoj ransomwaru: všechno to začalo s AIDS, Accessed on 2019-09.10.2019

https://www.antivirus.cz/Blog/Stranky/nejvetsi-kyberneticke-hrozby-roku-2018-ransomware-a-backdoory.aspx, (2018). Antivirus.cz, Největší kybernetické hrozby roku 2018 – ransomware a backdoory, Accessed on 2019-09.10.2019

https://www.antimalware.cz/blog/co-je-phishing (2019). Antimalware.cz, o je phishing, Accessed on 2019-09.10.2019

https://computerworld.cz/archiv/historie-hackingu-16840 (2001). Computerworld.cz, Historie hackingu, Accessed on 2019-09.10.2019

https://www.systemonline.cz/it-security/historie-soucasnost-a-budoucnost-dos-utoku.htm (2014). Systemonline.cz, Historie, současnost a budoucnost DoS útoků, Accessed on 2019-09.10.2019