SCIENTIFIC JOURNAL OF POLISH NAVAL ACADEMY

2019 (LX) 4 (219)

sciendo

DOI: 10.2478/sjpna-2019-0023

CYBERATTACK — EXAMPLES OF THREATS

Adam Stojałowski

Regional IT Centre, Strażacka 2-8 Str., 81-660 Gdynia, Poland; e-mail: a.stojalowski@gmail.com; ORCID ID 0000-0001-9503-8762

ABSTRACT

The purpose of this article is to present selected threats that may affect the security of IT systems caused by cyberattacks coming from cyberspace, as well as to prescribe the results that could be caused by the failure to implement security measures to protect information system (IS).

Keywords:
information and communication systems ICT, cyberattack, security threats, malicious code, TOR.

Research article

INTRODUCTION

Ensuring the required level of security of the information and communication system is a continuous process, which the current state depends on the adopted protection and selection of appropriate security mechanisms.

Commonly available studies, which can be easily found on the Internet, often contain ready-made guides presenting methods and manners of the attack information and communication systems. The mentioned studies may consist of properly prepared websites as well as videos posted on social networking sites available to the general public. Often, similarly as guides or films, Internet users place their own tips and information specifying the methods of attack. Marc Goodman describes this type of education in his publication as a kind of criminal university. *All of this training amounts to a sort of online criminal university (Crime U) that has accelerated the sophistication and skills of individual criminal hackers* [3].

Therefore, it is not difficult to assume that a significant group of people performing cyberattacks include users who do not have extensive IT knowledge and whose skills are based primarily on Internet resources.

In addition to the above mentioned wide group of Internet users, there are people or organisations whose activities can be classified as computer crime, both in terms of individual activities as well as teams carrying out organized and intentional attacks APT (Advanced Persistent Threat).

Most activities classified as cybercrime are carried out based on TOR (The Onion Router) networks resources. The aforementioned TOR network, created in 2004 by U.S. Naval Research Laboratory, in cooperation with Electronic Frontier Foundation and State Department [3], enabled communication of politically repressed people and fighting for democracy. Currently TOR network servers have mostly become a tool in the hands of cyber criminals. Sharing, selling stolen, counterfeit and illegal data as well as offering criminal services has now become synonymous with the TOR network.

In view of the threats listed above, people dealing with the security of information and communication systems must have a large amount of specialist knowledge. In this case, the selection of personnel responsible for security should be made in a considered manner and based on appropriate training and education. The knowledge of persons entrusted with tasks related to the security of information and communication systems should include both the ability to implement or apply protection methods, as well as knowledge of aspects related to cyberattack techniques.

COMPUTER SECURITY

Referring to the term ICT system security, it is necessary to present the related definitions:

Information Technology (IT) security or Information Communication Technology (ICT) security, is understood as a set of processes aimed at defining, achieving and maintaining the assumed level of confidentiality, integrity, availability, accountability, authenticity and reliability, i.e. security attributes in information and communication systems [1].

IT security management includes a set of processes aimed at achieving and maintaining an established required level of security, that means the level of confidentiality, integrity, availability, accountability, authenticity and reliability in information and communication systems [1].

The above definitions refer to attributes which determine the required level of security of information and communication systems. Lowering the level of any of the referenced security attributes results from the occurrence of events defined as security incidents.

Event: Any observable occurrence in a network or system [3].

Incident: An occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies [2].

The above quoted definitions of a security incident refer to events that may be as a result of unintentional or intentionally triggered factors. Events that occur as a result of intentional action can be categorized as a group of attacks against the security of the information and communication system.

Attack: An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system [5].

Cyber Attack: An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information [4].

EXAMPLES OF THREATS

Security of the information and communication system depends on the purpose of the system itself as well as the selection of adequate security mechanisms. Considering the example of an autonomous system, i.e. a system separated from local and external computer networks, it is assumed that the strong effort should be put on physical and procedural security aspects. A potential source of threats to the security of autonomous computer systems are errors resulting from bad or incorrect configuration, failure to follow the adopted procedures, as well as insufficient training of system users. Moreover, incidents related to computer infection are a frequent cause of violation of the security of autonomous systems. In relation to separated systems, incidents related to malicious code infection occur as a result of connecting external data carriers such as CDs, DVDs or portable USB flash drives. A necessary condition to minimize the probability of infection of the operating system is the use of anti-virus protection. In addition, each OS, including those operating in autonomous systems, must be periodically updated. In order to minimize the likelihood of computer infection, it is necessary to follow the rule of downloading updates only from reliable repositories, available in the resources of the appropriate software vendor.

The security of systems using network communication is considered differently in particular systems having an Internet access. In this case, in addition to physical or procedural security, an important role is played by the proper selection of measures to protect against unwanted and dangerous network traffic. Effort should also include monitoring and effective analysis of events.

Source of the attack

For the purpose of this article, presented data coming from an dedicated ICT system. The discussed system implements mechanisms prepared for monitoring unwanted traffic originating from the Internet. Moreover, the system configuration enables recording security break attempts and correlating events based on the characteristics of packet transmission.

Placed below pictures present an analysis of packet transmission, the aim of which was to break the security of the ICT system. Next, there are presented lists of IP addresses from which a brute-force attack was carried out.

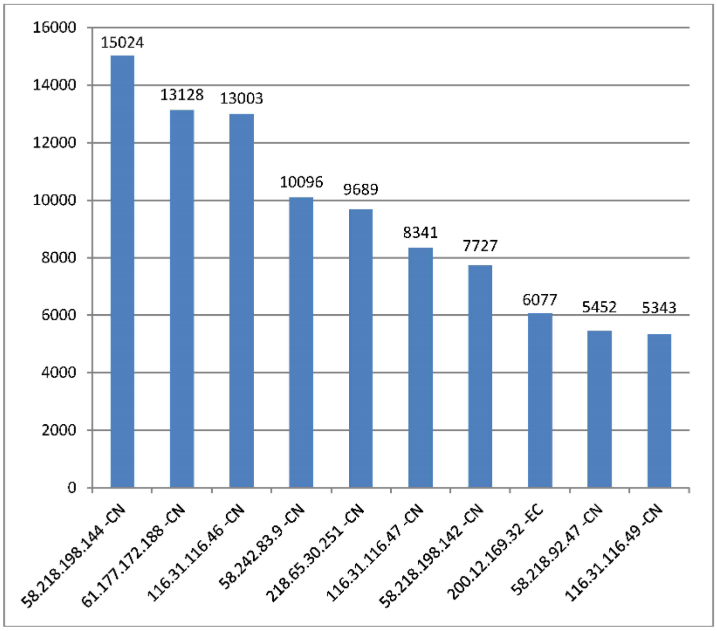


Fig. 1. Top 10 IP addresses (system graph view)

The chart contains IP addresses and codes of countries from which attempts of force attacks were made, presented in the form of the number of occurrences. The highest number of events was generated from the IP address 58.218.198.144, coming from the People's Republic of China.

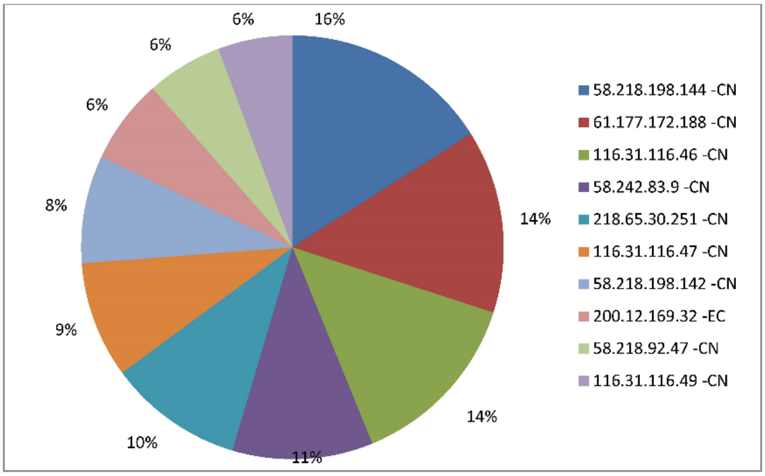


Fig. 2. Top 10 IP addresses — percentage value (system chart view)

The system also allows to read geographical coordinates (Latitude, Longitude) of IP addresses from which the attack was carried out.

Tab. 1. Top 10 IP addresses — tabular overview (system tabular view)

IP Address	Probes	City	Region	Country Name	Code	Latitude	Longitude	Hostname
58.218.198.144	15024	Nanjing	Jiangsu Sheng	China	CN	32.0617	118.7778	58.218.198.144
61.177.172.188	13128	Nanjing	Jiangsu Sheng	China	CN	32.0617	118.7778	61.177.172.188
116.31.116.46	13003	Guangzhou	Guangdong	China	CN	23.1167	113.25	116.31.116.46
58.242.83.9	10096	Hefei	Anhui Sheng	China	CN	31.8639	117.2808	58.242.83.9
218.65.30.251	9689	Nanchang	Jiangxi Sheng	China	CN	28.55	115.9333	251.30.65.218.broad.xy.jx.dynamic.163data.com.cn
116.31.116.47	8341	Guangzhou	Guangdong	China	CN	23.1167	113.25	116.31.116.47
58.218.198.142	7727	Nanjing	Jiangsu Sheng	China	CN	32.0617	118.7778	58.218.198.142
200.12.169.32	6077	Quito	Provincia de Pichincha	Ecuador	EC	-0.2167	-78.5	200.12.169.32
58.218.92.47	5452	Nanjing	Jiangsu Sheng	China	CN	32.0617	118.7778	58.218.92.47
116.31.116.49	5343	Guangzhou	Guangdong	China	CN	23.1167	113.25	116.31.116.49

The analysis of the reports shows that about 92% of the network traffic of the analysed system originates from the People's Republic of China. However, it cannot be excluded that most of these addresses are not a real source of attack. There is a high probability that the IP addresses presented are used as a false source using the IP spoofing method or by using proxy servers.

It can also be assumed that a significant number of attacks originate from IP addresses that are only used for cybercrime purposes in the Internet. These addresses are part of the TOR network, mentioned earlier in the article.

Analysis of the chosen attack

Brute force attacks presented in the previous part of the article were aimed at breaking the security of the ICT system and, as a consequence, implementing a malicious code by the attacker. Presented below examples show methods of malicious code installation as a result of breaking security in a compromised ICT system.
The first example is presenting operations being aimed at execution:

- attempts to disable the local firewall;
- attempts of the installation of the malicious code;
- attempt to change attributes and modify the file.

```
server:~# iptables stop
server:~# wget -O /tmp/Ceo http://222.186.57.232:8080/Ceo
http:///tmp/Ceo: Unsupported scheme.
server:~# chmod 0777 /tmp/Ceo
server:~# nohup /tmp/Ceo> /dev/null 2>&1 &
bash: nohup: command not found
server:~#
```

Fig. 3. Attempting to install malware of type backdoor (system log analysis)

Performing the operation of downloading the software from the address http://222.186.57.232:8080 was aimed at installing malicious software which is classified as a backdoor. This kind of backdoor spreads via shared networks or attaches itself to downloadable files. That malicious software is classified as a backdoor infection, because it can easily bypass to computer.

The next example shows the operations performed by the attacker after gaining access to the system.

- attempt to disable the local firewall;
- attempts of the installation of the malicious code;
- attempt to change attributes and modify the file;
- attempt to keep the malicious code working after log off;
- cleaning history.

```
server:~# iptables stop
bash: iptables: command not found
server:~# wget -O /tmp/vjudp http://183.61.171.149:5896/vjudp
http:///tmp/vjudp: Unsupported scheme.
server:~# wget -O /tmp/vjudp http://183.61.171.149:5896/vjudp
http:///tmp/vjudp: Unsupported scheme.
server:~# chmod +x /tmp/vjudp
server:~# nohup /tmp/vjudp > /dev/null 2>&1 &
bash: nohup: command not found
server:~# chmod 0755 /usr/bin/nohup
server:~# ls
server:~# ls-la
bash: ls-la: command not found
server:~# pwd
/root
server:~# cd root
bash: cd: root: No such file or directory
server:~# cd /root/
server:~# history -c
server:~# pwd
/root
server:~#
```

Fig. 4. Attempting to install malware of type trojan Linux/Setag.B.Gen (system log analysis)

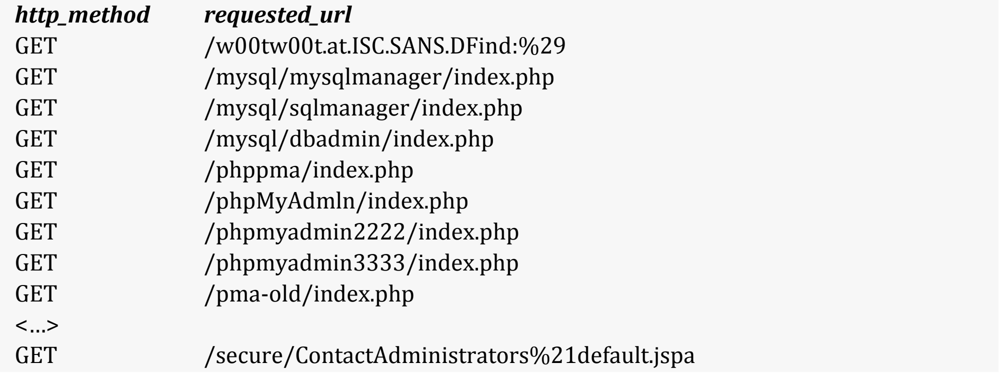
This example belongs to a group of complex attacks. Also in this case, the attacker tried to install malware of the type trojan.

Linux/Setag.B.Gen is backdoor that arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites. It executes commands from a remote malicious user, effectively compromising the affected system. It connects to certain websites to send and receive information [6]. In addition, this malicious code perform a lot of harmful activities in the system background. It can also bypass antivirus programs making system vulnerable and collect sensitive data such as username, password or email addresses.

Web server threats

The next part of the article will present an analysis of one of the attack on a web server. The following example illustrates the steps taken by a hacker to break security and modify or steal processed data.

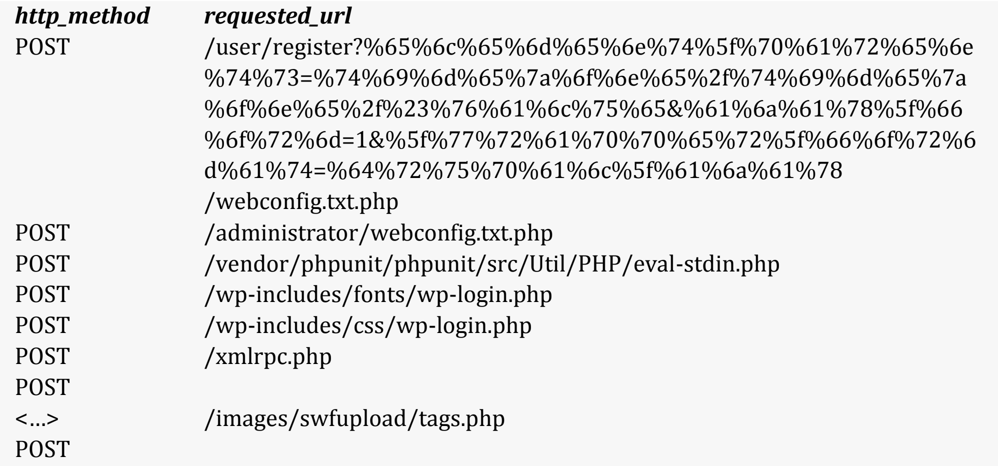
First of all, the adversary performs a reconnaissance of the service and performs scan of the server to find out of its vulnerabilities. The details are presented in the fig. 5. For this purpose, the parameters are transferred to the server using the GET method. The figure below also presents an attempt to obtain information from the MySQL database using the PMA tool (phpMyAdmin) in various possible configuration variants.



```
http_method     requested_url
GET             /w00tw00t.at.ISC.SANS.DFind:%29
GET             /mysql/mysqlmanager/index.php
GET             /mysql/sqlmanager/index.php
GET             /mysql/dbadmin/index.php
GET             /phppma/index.php
GET             /phpMyAdmln/index.php
GET             /phpmyadmin2222/index.php
GET             /phpmyadmin3333/index.php
GET             /pma-old/index.php
<…>
GET             /secure/ContactAdministrators%21default.jspa
```

Fig. 5. Web server reconnaissance (system log analysis)

In the next part of the attack, the adversary communicates with the server by sending requests using the POST method. Selected events are presented in the fig. 6. There are various types of attempts to interfere in the service environment.



```
http_method     requested_url
POST            /user/register?%65%6c%65%6d%65%6e%74%5f%70%61%72%65%6e
                %74%73=%74%69%6d%65%7a%6f%6e%65%2f%74%69%6d%65%7a
                %6f%6e%65%2f%23%76%61%6c%75%65&%61%6a%61%78%5f%66
                %6f%72%6d=1&%5f%77%72%61%70%70%65%72%5f%66%6f%72%6
                d%61%74=%64%72%75%70%61%6c%5f%61%6a%61%78
                /webconfig.txt.php
POST            /administrator/webconfig.txt.php
POST            /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
POST            /wp-includes/fonts/wp-login.php
POST            /wp-includes/css/wp-login.php
POST            /xmlrpc.php
POST
<…>             /images/swfupload/tags.php
POST
```

Fig. 6. Web server attack (system log analysis)

The analysis of the above events confirms the necessity of using mechanisms that prevent the acquisition of sensitive data. In order to do this, it is necessary to protect and prevent access to configuration files. It is also recommended to use tools to monitor and block unwanted traffic by implementing programs like Web Application Firewall (WAF).

CONCLUSIONS

Maintaining the assumed level of security of the information and communication system is a process that requires continuous analysis of events and response to incidents. A prerequisite for effective protection of the system having access to the Internet is the implementation of the required security components, which primarily include the firewall and antivirus protection. It is also an added value that the system administrators have the required knowledge of how to manage safety mechanisms. These factors are elements of the security policy, which in turn is defined as a set of accepted rules in order to ensure the required level of security and protection of data processed in ICT systems.

The security policy is defined as a plan or method of action adopted to ensure system security and data protection. It expresses a set of rules that determines what should be protected, how and why ICT systems should serve the tasks faced by the institution [1].

Despite the use of increasingly sophisticated methods of protection, a number of growing threats are observed, particularly in relation to these ICT systems which, due to their intended use, must have permanent access to the Internet. Attack methods are constantly evolving. As an example one can refer to malware categorise as ransomware, which indicates the date of initiation of one of the most dangerous Trojans called CryptoLocker [5] on day 5 September 2013, has undergone a number of modifications. The first appearances of software type ransomware were accompanied by noticeable errors in the content of the e-mail sent. At present, people who commit this kind of computer crime use very advanced mechanisms that often use social engineering methods.

Taking the above into account, it is worth returning to the methods that the users of ICT systems have seen in recent years as a waste of time. Here it is considered trainings in the field of information and communication system security that conducted in a thoughtful manner, can bring immeasurable results, often exceeding specialized and very expensive security measures.

REFERENCES

[1] Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Publ. WNT, Warszawa 2007, pp. 10, 33, 43 [*Information and services security within modern organizations and probabilities* — available in Polish].

[2] *Committee on National Security Systems (CNSS) Glossary*, CNSSI No. 4009, April 2015, pp. 50, 61.

[3] Goodman M., *Zbrodnie przyszłości. Jak cyberprzestępcy, korporacje i państwa mogą używać technologii przeciwko tobie*, Publ. Helion, Gliwice 2016, pp. 208, 222 [*Future Crimes: Everything is Connected, Everyone is Vulnerable* — available in Polish].

[4] *NIST Special Publication 800-39*, National Institute of Standard and Technology, Managing Information Security Risk Organization, Mission and Information System View, Information Security, March 2011, pp. B-1.

[5] *Ransom.Cryptolocker*, [online], https://www.symantec.com/security-center/writeup/2013-091122-3112-99 [access 05.09.2019].

[6] Shirey R., *Internet Security Glossary, IETF 2000, RFC 2828*, [online], https://www.rfc-editor.org/rfc/rfc2828.txt [access 18.03.2019].

[7] *Trend Micro*, [online], https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/backdoor.linux.setag.rpb [access 05.09.2019].

CYBERATAK — PRZYKŁADY ZAGROŻEŃ

STRESZCZENIE

Celem artykułu jest przedstawienie wybranych zagrożeń wpływających na bezpieczeństwo systemów teleinformatycznych powodowanych przez ataki pochodzące z cyberprzestrzeni, a także pokazanie skutków, jakie mogą być następstwem zaniechania implementacji środków bezpieczeństwa w celu ochrony systemów teleinformatycznych.

Słowa kluczowe:
bezpieczeństwo systemu teleinformatycznego, cyberatak, zagrożenia systemu teleinformatycznego, TOR.

Article history
Received: 25.03.2019
Reviewed: 21.06.2019
Revised: 26.11.2019
Accepted: 09.12.2019