JOURNAL OF SCIENCE OF THE MILITARY ACADEMY OF LAND FORCES

Volume 49 Number 2 (184) 2017 ISSN 1731-8157

DOI:

CYBER ATTACKS AND THREATS

Marek WITKOWSKI[*], Anna WOJACZEK[*]

[*] *The Faculty of Management, General Tadeusz Kosciuszko Military Academy of Land Forces in Wroclaw*
e-mail: m.witkowski@wso.wroc.pl
e-mail: a.wojaczek@ wso.wroc.pl

Received on 15th April ; accepted after revision September 2016

Abstract:

The article presents current threats and examples of malware which can be used to disrupt the infrastructure. Next, a classification of current threats and attacks which occur in cyberspace is proposed. Finally, the publication also presents examples of attacks which disrupted the smooth functioning of networks and systems.

Keywords:

cyberterrorism, cyber threats, terrorism network, Information and Communication Technology (ICT) systems

INTRODUCTION

The goal of this article is the presentation of current threats and possible attacks on IT systems. An analysis of attacks carried out using the Internet shows a growing threat to the security of data sent and stored in IT systems and equipment. The danger of losing such information refers not only to state organisations and institutions, but it can also pose a threat to private entrepreneurs and individual users. This is why all computer users, especially the ones connected to local or global networks, should realise the danger so as to protect themselves. Even basic safety measures introduced to secure internet connections can efficiently protect data from unauthorised access.

1. CYBER THREATS

The use of modern IT technologies results in extensive development of services and practically unlimited access to global information. However, this situation has also led to an increase in possible threats connected with the above mentioned factors. Hence, there is a legitimate need to make the users of IT systems aware of existing threats and to inform them about attacks on IT systems. Better awareness of the threats occurring in the network-centric environment will help them to understand the need to protect sent or stored data from unauthorised modification or theft. Due to the fact that ICT systems are used in nearly every area of human activity, there is a need to protect sent information [2]. One of the basic Internet threats is cyberterrorism, cyber espionage and cybercrime. The doctrine on cybersecurity of the Republic of Poland of 2015 indicates that cyber espionage is an important external threat in cyberspace. This type of espionage is strictly connected with actions conducted by foreign intelligence services, non-government entities and terrorist organisations which use specialist tools to gain IT resources. Collected data can be used by criminals to gain access to sensitive materials, which can lead to interference with state structures functioning [1]. Such a situation makes "computerised" users protect their equipment, networks and ICT systems.

The above mentioned networks and systems with their peripherals together make ICT infrastructure which should be particularly protected. Its efficient operation ensures the proper functioning of all elements responsible for the security of the state, including international structures. Incorrect operation of particular elements of an integrated system can have an adverse effect on the other components of the integrated system and in consequence it can interfere with the information flow in emergency situations.

Pursuant to the constitutional provisions of the Republic of Poland and other legal documents, the state is obliged to ensure external and internal security. Taking cyberterrorism into account, the task becomes more difficult to achieve as there are no defined limits for this criminal activity. Hence, most of terrorist activity in cyberspace remains beyond state control. Interference with the operation of critical state infrastructure and possible attack on any of its elements can lead to limiting the efficiency of its operation [3]. The sources of threats in cyberspace are mainly extremist and terrorist organisations as well as transnational organized crime groups whose attacks in cyberspace can be conducted for ideological, political, religious, business and criminal reasons [1]. The characteristics and examples of potential threats and Internet attacks are presented in the further sections of this article.

2. MALWARE

The notion of malware is understood as any kind of applications or scripts which can be intentionally used by hackers to affect ICT systems so as to interfere with their operation, incapacitate them or destroy resources stored in them or for financial gains.

According to generally available literature and materials collected by the Authors of this publication, malware encompasses:

- Viruses – they need the so called host, it can software or a hard drive, to be active and to replicated without user's consent. Viruses can be divided into e.g. file, macro, email, BIOS, polymorphic viruses;
- Worms – contrary to viruses, they replicate and propagate by themselves, very frequently using email. A good example can be the Web Worm which is hidden in the code of a specially prepared website;

- Hoaxes – they sent false information to users of Internet connections. Usually these are alarms related to computers allegedly infected with dangerous viruses which can delete use data and make further work on a given computer impossible. Together with the above information they also send a programme which can remove malware. In consequence, when such a programme is installed, important system files are deleted. After an attempt to reboot a computer, it turns out that its operating system cannot be started due to the lack of these files;
- Wabbit – it is activated in the backstage. It is not replicated in a network and it does not attack any software either, it self-replicates. An example of wabbit is a fork bomb which multiplies operating system processes until all available resources are exhausted;
- Trojan horses – programmes which seem to be useful, but in fact perform such actions as stealing passwords, downloading viruses from the net, spying, opening ports, deleting data. Common Trojans allow to take over control of a computer and consequently have access to data stored on a hard drive and remotely control an infected device. An example of such programme is Cryptolocker, an application which allows to encrypt files in infected computers. Trojan horses have very efficient encryption algorithms, this is why a user has to pay a significant amount of money (about 3000 EUR) to regain access to blocked files thanks to a special password he/she receives;
- Backdoor – programmes which allow to gain repeated, unauthorised access to a computer from the Internet. They use a previously created gap in security;
- Exploits – their goals is the same as that of backdoors. They use existing gaps in the operation system, software and network services, etc. ;
- Rootkits – their presence is hidden in the system (files, processes) until they enable unauthorised access and total control of an infected computer;
- Spyware – spying software which collects and sends various types of information: user passwords, credit card numbers, etc.;
- Adware – software responsible for presentation of advertisements, very frequently it infringes user privacy by monitoring websites visited by them;
- Diallers – they can attack only computers connected to the Internet with a modem. They do not affect computers with wideband Internet access. They dial telephone lines using the access number very frequently incurring expensive bills much higher than typical Internet access costs (foreign or commercial telephone lines);
- Hijackers – they force connections with a particular Internet service, e.g. by altering Internet browser settings;
- Keyloggers – programmes which recognize and record keystrokes of a user to later disclose passwords and other information. Additionally such pro-

grammes record web addresses at which users passwords were used. A file with the above information is automatically sent to an indicated email address. There are also hardware keyloggers.

3. INTERNET ATTACKS

In computer networks an attack is any attempt to destroy, steal, modify, block or gain unauthorised access to some resources.

To the best of their knowledge and on the basis of collected research materials, the Authors propose to include the following attacks in this group:

- spoofing – masquerading as another computer in a network. Traditionally, spoofing referred to the process of gaining access rights from one computer to another by falsifying data packages and using this to “imitate” a trusted host. Currently it means any way of breaking computer security authorisation based on the host address or its name. An example of spoofing is DNS-spoofing, i.e. imitating a DNS server. In such an attack DNS server responses related to IP addresses relations with domain names are falsified. It is necessary to create a fake DNS server in the net which will search for enquiries about name mapping and will related them with false IP addresses. Due to the fact that the fake server has to pre-empt communication with the real one, the operation of the latter is slowed down or even completely blocked (e.g. using a DoS attack).

DNS-spoofing allows to gain unauthorised access to confidential data by phishing, redirecting a user to any type of a fake website which looks delusively similar to the original one. Such attacks are very often aimed at electronic banking.

Another example is ARP-spoofing (ARP-poisoning), in this case fake ARP-Reply packets are sent (on their basis computers connected to the net receive information on IP addresses mapping to physical addresses), this allows to pose as a computer in LAN and hence gaining access to data. A scheme of an ARP-spoofing attack is presented below:

- computer A – sender;
- computer B – attacker;
- computer C – receiver.

1. (A) Sending an ARP request for the IP address 192.168.0.13;
2. (B) Sending a reply – this is my address 00:40:C8:D2:51:BB.
3. (A) Adding a dynamic ARP entry – IP address 192.168.0.13 to MAC

   00:40:C8:D2:51:BB.
4. Communication between A and computer B;
5. (B) Sending an ARP request for the IP address IP 192.168.0.13;
6. (C) Sending a reply – this is my address 00:40:F2:AA:51:12;

7. (B) Adding a dynamic ARP entry – IP address 192.168.0.13 to MAC 00:40:F2:AA:51:12;
8. Computer B transfers the information from computer A to computer C (the real addressee).

It is very important to send a request for the IP address of the real addressee (point 5) and transfer the information the information received from the sender to this address (point 8). Then the communication between the sender and the attacker can remain unnoticed.

- sniffing – it is gaining access to data sent between computers in a LAN. Classical sniffing was related to networks using a coaxial cable or hubs. In such networks data were sent to all connected computers and they were processed only by those to which they were addressed. Simultaneously it was possible to place the Internet interface card into a promiscuous mode which allowed to capture all data sent in a given LAN, not only the ones sent to a particular computer. Currently sniffing requires using other methods, e.g. ARP-spoofing;
- phishing – it is a method allowing to gain unauthorised access to information by posing as trusted institutions, e.g. banks. A more advanced and hence, more difficult to detect version of this attack is pharming which frequently uses DNS-spoofing. During such an attack a user can be sent a message which can be considered authentic. Most often these messages are allegedly sent by well-known banks or companies, there is also a link to a phishing website;
- spamming – sending email users unwanted trade offers they did not order. The largest number of such mails comes from the United States (about 10% of total spam). The second highest ranked country is Vietnam (7%) and Ukraine (6.8%) [5];
- DoS (Denial of Service) – this attack is aimed at the availability of data and services. The server which is a victim of such an attack is flooded with an excessive number of requests, which results in blocking the service or its significant slowdown. It is also possible to take advantage of an error causing malfunction. A classical attack of this type is Ping of Death in which data packets larger than the admissible size are sent as part of TCP/IP service called Ping. Currently an improved version of this attack is used, namely DdoS (Distributed Denial of Service) conducted simultaneously from many places, which results in increased force of such violation. An example of a DoS attack is *SMB-nuke*. Especially the Microsoft Windows operating system with active NetBIOS service – Network Basic Input/Output System are prone to such attacks. It ensures connection between an application interface and other computers as well as data sharing. NetBIOS transmitted in TCP/IP (currently the most popular method) uses the following ports: 137, 138 and 139 which must be open to conduct an attack.

During a *SMBnuke* attack an appropriate Internet frame with an SMB protocol packet (Server Message Block – protocol allowing to offer access to resources, e.g. files and printers) is sent, it causes a computer restart.

Another version of this attack – *SMBnuke v.2* – uses an error in SMB client message interpretation, which results in a system freeze.

One more example is *UDP flood* which employs the User Datagram Protocol (UDP) used by some applications instead of TCP for faster and simpler (and hence also less reliable) data transfer between hosts. In a *UDP flood* attack a large number of UDP packages are sent to the ports of an attacked system. The system searches for an application waiting on the target port. When it cannot be found, an ICMP packet is generated (ICMP is a service protocol which reports connection errors between hosts), it is then sent to the IP source address. For obvious reasons this address is falsified by an attacker. If a sufficiently large number of UDP packets is sent to the ports of the attacked system (which as a result is forced to send a large number of ICMP packets) a DoS of the victim system takes place.

Botnet attacks – botnet is a network of computers controlled by other people as a result of infecting them with malware (e.g. worms, Trojans) without the consent of their owners. This type of attack allows to remotely control a device. Such an infected computer is commonly called a zombie computer.

Such networks can be used for various types of IT crime, DDoS attacks, spamming, distributing malware, adware installation and other types of malicious software. An example of botnet is Storm (detected for the first time in January 2007), developed by a Trojan horse called *Storm Worm* which infects Microsoft Windows. Usually these attacks take advantage of gaps in security systems or in applications installed in them. The name botnet originates from the title of the first messages which were used to distribute *Storm Worm*: “230 dead as storm batters Europe”. After opening an attachment to this email, a computer was infected. Later there were emails looking as if sent from well-known producers of anti-virus software with false links to various services (e.g. YouTube) and e-cards. However, the main idea of such attacks remained the same. It is estimated that at the peak of its activity Storm-botnet infected one million of computers [6]. According to some other sources, even two million computers were attacked and the total share in spam sent all over the world was 20%. Another known botnet is e.g. *Bredlab* which attacked Facebook, *Zeus* which stole bank passwords and IDs as well as other data, *Waledac* which earned an opinion of being one of the most efficient spam sending tools, *Mariposa* which attacked over 13 million computers in 190 countries, it stole data, e.g. credit card numbers.

4. OTHER THREATS

Except for the above mentioned examples, one should also take into account following threats:

a) Computer equipment faults which most often are caused by:

– interference from electric current caused by lightning discharges, wrong power supply parameters, power supply surge and faults;

- mechanical faults of particular computer components;
- consequences intentional or unintentional activity of a user or other people (e.g. spilling a drink on a computer, a fire., etc.).

a) Data carrier faults – they occur mainly due to incorrect use (e.g. storage in places where they are exposed to sunlight or very high or low temperatures);

b) Data faults – an example of such a hacker tool is *Rombertik* which is a variant of blastware. The tool has a self-destruction function, when it is detected it destroys hard drive data. It can infect a computer when downloading mail with a pdf attachment which after opening becomes an executable file for Windows. When *Rombertik* is installed in the operating system, it captures data stored on a computer and passwords in Internet browsers. Moreover, it can be detected in a browser and next it can copy data entered in portal forms using HTTPS, used e.g. by bank websites;

c) Physical access to equipment and services by unauthorised people –direct access to a computer of third persons with simultaneous use of poor security, in practice offers unlimited opportunities to gain access to data stored in such systems, mainly logins and passwords of all users;

d) Equipment theft – a significant problem, especially in the case of laptops and data carriers.

5. CLASSIFICATION OF ATTACKS

Taking into account attack elements as the basis for classification, the following division of attacks is possible:

- Probe – attempts to gain access to a particular object by analysing its characteristics;
- Scan – it is conducted for many objects to check their accessibility and then uses their susceptibility;
- Flood – causing situations in which processing capabilities of a given object are exceeded;
- Read – unauthorised access to information with read authorisation;
- Copy – unauthorised access to information to copy data;
- Modify – changes in the characteristics/content of an attacked object;
- Steal – gaining access to particular resources by an unauthorised person (without leaving their copies);
- Delete – destruction of an attacked object;

- Spoof – posing as a system element or a user authorised to access a given resource;
- Bypass – overcoming security by using an alternative way of gaining access to an object.

6. EXAMPLES OF CYBER-ATTACKS

The above presented threats allow to conduct a cyberattack of not only one computer but also whole systems and organisations. One of the most serious cyberattacks was the attack on Estonia which took place in May 2007. The websites and servers of the most important state institutions were infected. The Estonian society suffered chaos and fear for over 20 days. The consequence of this very well planned action was showing the weaknesses of IT systems which were supposed to guarantee the security of the state and its citizens.

In June 2015 a hacker known as Raz broke into the IT system of Plus Bank and requested PLN 200,000 for keeping all the information about bank customers confidential. The problem was revealed when the offender did not receive his ransom and uploaded the information that for a few months he had had unlimited access the IT system of Plus Bank. In consequence he managed to rob an undefined number of people and to steal nearly the whole database of individual and corporate clients as well as webserver files. Because Plus Bank did not pay the amount of money requested by the offender, he started to publish data about customers. The published data encompassed such information as:

- name and surname;
- e-mail address;
- address;
- PESEL (personal ID number in Poland);
- ID card number;
- History of the last 50 bank transactions;
- Information about deposits and loans [7].

Another example of cyberterrorism was an attack on IT resources in Georgia in 2008. The goal of attacks were mainly government services as well as banks, the foreign embassies of the countries supporting Georgia. This campaign was a classic DDoS and was coordinated by services related to underground organisations conducting criminal activity on the Internet (most of them were connected with RBN – the Russian Business Network [8]). An interesting fact about this DDoS attack was the fact that websites and blogs invited anyone to participate in the attack. There were instructions and software necessary to join in, it could be done by anyone with Internet access. No professional knowledge was required to participate in the attack.

One more example worth mentioning here is the use of a virus called *Stuxnet*, which infected Iranian systems. Actually it attacked nearly the whole infrastructure of this country, however, the main goal was the ICT system of a nuclear power plant in Iran. The virus took total control over the computer system in the power plant leading to its complete paralysis. At the same time oil pipelines and even military systems were also attacked. The *Stuxneta* attack was one of the most complex and complicated attempts to take control of critical infrastructure in the history of cyber threats.

The fact that nobody can feel safe is confirmed by the following example. Cybercriminals managed to steal top secret documentation of the US intelligence, which shows that the USA, regardless of numerous attacks on their state and private computer systems, cannot solve this problem. The attacked institution was the department keeping the data of American spies and other military staff (the so called section 86). Hackers gained access to such data as: detailed reports including social security numbers, access to classified information, information on loans, addictions and mental diseases. There were the data of very important agents and civilian employees of key significance for the state employed at the NSA, CIA, special military units and intelligence services. Gaining access to the above information can be pose threat to the lives of the intelligence agents because hackers can sell the data spies working in foreign countries, which in consequence can lead to their dismissal from their current jobs [9].

On August 14-17, 2014 DDoS attacks were conducted on *www.prezydent.pl* and *www.gpw.pl* and other state administration portals. The organisation which claimed responsibility for the attacks used the name “CyberBerkut” on their website, the reason was the alleged involvement of Poland in the conflict in Ukraine. During the attacks a large number of synchronisation requests were sent to the server, this kind of attack is called SYN FLOOD. It results in the saturation of server resources. Access to portals is denied because the attacked website receives a large number of packets sent in a very short time [4] .

Except for the above described DDoS attack, the Warsaw Stock Exchange was attacked again on 23 October 2014. Its website *www.gpwcatalyst.pl* was replaced by a fake one with an image of jihadists and an inscription which read “TO BE CONTINUED...” [4].

There was also a cyberattack during the regional elections in 2014. Its target were the servers of the National Election Office. The hackers gained access to information about the structure of the system database and this allowed them to publish the data on the Internet. The information encompassed such data as email addresses, cryptographic hash functions, logins, names and surnames [4].

These and other attacks described earlier, whose number keeps growing every year as well as their possible consequences show to what extent the world today is dependent on technology and how dangerous this is to the security of the state and the society.

Finally it is worth mentioning the most important comments from the CERT POLSKA 2014 report:

- It can be concluded that on average about 280 thousand computers are infected in Poland;

- Although Poland is not the main target of the attacks of the Advanced Persistent Threat (APT), some incidents of this type have been reported, e.g. *Pawn Storm* and *Energetic Bear*;
- An increase in threats directed at e-banking users. The value of stolen funds sometime reached even several hundred thousand PLN. The most common bank Trojans are: *Kronos*, *VMZeuS*, *ISFB* and *Tinba*;
- An increase in the number of attacks on regional governments and corporate clients has also been observed;
- The SSDP dominates in wrongly configured infrastructure;
- Phishing methods development can still be observed. There is an increasing number of attacks on online games and fiscal administration, apart from such traditional targets as banking and financial services;
- The most significant problem of data breach was related to the Warsaw Stock Exchange;
- DDoS attacks are conducted mainly in e-commerce and public administration portals and services;
- *ZeuS* and *Zero-Access botnets* increased their share in infected computers. Besides *Confickera* they are the boggest botnets in Polish networks.

CONCLUSIONS

The goal of this publication was the presentation of current threats and attacks which can interfere with the operation of ICT systems. The article showed various aspects and the dynamics of contemporary threats, which can significantly influence the operation of IT systems and the security level in cyberspace.

The list of potential threats is growing and it is evolving towards more and more complex solutions, which will allow not only to capture data, but also to modify or delete them. Moreover, this kind of software combined with professional knowledge of a hacker can lead to remotely taking control of a computer, any other multimedia device or even the whole ICT system.

Hence, all users should know that firewalls, antispyware and antivirus software are not the only ways of ensuring the security of computer and Internet use. It is equally important for the users to have basic knowledge about potential threats and be able to protect their from intentional or intentional attacks at least at a minimum level. Certainly together with an increase in user awareness, the level of ICT services security will also grow.

REFERENCES

1. Cybersecurity Doctrine of the Republic of Poland, Warszawa 2015.
2. Górka M., Cyberbezpieczeństwo, jako bezpieczeństwo państwa i społeczeństwa

w XXI wieku, Difin, Warszawa 2014.

3. Podraza A., Potakowski P., Wiak K., Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna, Difin, Warszawa 2013.
4. Report on Cybersecurity of the Republic of Poland 2014, Warszawa 2014.
5. [online], Available on the Internet: http://www .chip.pl/news/ bezpieczenstwo /wirusy/2015/05/parszywa-dwunastka-spamerow-w-2015-rok.
6. [online], Available on the Internet http://www.idg.pl/news/148781/microsoft .zalatwilismy.storma.html.
7. [online], Available on the Internet: http://softonet. pl/publikacje/aktualnosci /Plus Bank.nie.spelnil.zadan.hakera.wyciekly.dane.klientow,954.
8. [online], Available on the Internet: https://www.cybsecurity.org /gruzja-rosja-konflikt -w-cyberprzestrzeni.
9. [online], Available on the Internet: http://technowinki.onet.pl/internet-i-sieci /hakerzy -wykradli -dane-amerykanskich-szpiegow/l872m2.

BIOGRAPHICAL NOTES

MAJ Marek WITKOWSKI – PhD, the author and coauthor of over 20 scientific publications on broadly understood computer science and security systems. His main area of interest are Communication and IT equipment development trends.

LT Anna WOJACZEK – MSc, a lecturer, currently at The Faculty of Management, General Tadeusz Kosciuszko Military Academy of Land Forces in Wroclaw.

HOW TO CITE THIS PAPER

Witkowski M., Wojaczek A., (2017). Cyber attacks and threats. *Zeszyty Naukowe Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. Tadeusza Kościuszki Journal of Science of the gen. Tadeusz Kosciuszko Military Academy of Land Forces*, 49 (2), p. 184-194, http://dx.doi.org /10.5604/17318157.1221843