VANJA KORAĆ
Mathematical Institute SASA
Belgrade, Serbia
E-mail: vanja@mi.sanu.ac.rs

DRAGAN PRLJA
Institute for Comparative Law
Belgrade, Serbia

343.85::004.056.53
COBISS.SR-ID 272049676
Original research article

Received: October 14th 2018
Accepted: October 30th 2018

TARGETING CYBER THREATS BY RECOGNIZING ACTIVE AND PASSIVE MALICIOUS ATTACK TECHNIQUES AND PROTECTING INFORMATION

ABSTRACT

Attack techniques recognised in digital forensic practice and used by malicious attackers to break into a system will be described in this paper. The aim of this paper is to raise security awareness in users who are working in the Internet environment both at their organisation and at home. Measures of defence and possibilities of protection from the security challenges presented in this text will also be proposed in this work.

KEYWORDS: CYBER THREATS, SYSTEM PROTECTION, PROTECTION AGAINST ATTACKS.

Digital wellbeing is the most important thing in an organisation. For this reason, organisations are investing heavily in the protection of their systems.[1] Nowadays, it can be said that it has become a real security challenge to protect sensitive information from the competition. The competition today represents one of the most important reasons for protecting information in organisations. The novelty with regard to obtaining a competitor's information is the possibility of renting malicious attacks to steal important information (for example, business plans for a particular quarter). The competition may subsequently take advantage of these stolen pieces of information. With the emergence and expansion of the Internet, an increase in the number of interconnected devices has also led to an uncontrolled increase in the number of Internet of Things (IOT) devices. On the other hand, it has created conditions to increase the speed, number, and scope of cyber attacks. At the same time, competitive organisations tend to increase their quality of service, and increasing the quality of service also demands faster delivery of services or products. Subsequently, this has lowered the level of security, as insufficient attention is given to this subject, as this would require allowing more time to perform detailed security checks.

In literature, a malicious attacker is often equated with a hacker, but this is not totally precise. The term hacker was applied to people who are engaged in research and the development of protection for the benefit of the Community. Over time, with the possibility of extra earnings and with the increasing number of devices on the Internet, this term began to have a negative con-

1 The article results from the project *IRS - Viminacium, Roman city and military legion camp – research of the material and nonmaterial culture of inhabitants by using the modern technologies of remote detection, geophysics, GIS, digitalization and 3D visualization* (*no 47018*), funded by the Ministry of Education, Science and Technological Development of the Republic of Serbia.

notation, marking it as malicious, because certain individuals (hackers) directed their knowledge towards committing malicious attacks. The latest trend includes associations of hackers, i.e., the forming of hacker communities that have excellent informatics knowledge and skills in different fields (social engineering, hacking with the aim of compromising computer systems, post exploitation techniques). Depending on the motives and goals that trigger the hacker activity, and for the purpose of terminological demarcation, the most common division found in the literature is the following (Lanier 2018):

Black hat – these malicious hackers, i.e., malicious attackers, are motivated by financial gain and they are solely engaged in malicious activities for mercenary reasons. They break into computer systems and networks, misuse vulnerabilities on computer systems, steal user credentials, release confidential government or business documents, and spread malicious and ransomware programmes.

White hat –this type of hacking activity is also called ethical hacking and can be performed by persons employed in companies in the position of Chief Information Security Officer (CISO) or by consultants in the field who actually explore the vulnerabilities in the computer and network systems of their organisations with the aim of implementing the best possible protection.

Grey hat–this type of hacker performs the same activities as the white hat, until the moment when financial gain becomes crucial.

Script kiddie –these types of hacker activities are mainly performed by beginners hacking for entertainment or to prove themselves. In order to raise their rating as hackers they must have certain hacker experience behind them. To achieve superior hacking skills, it is necessary to gain access to certain forums or sites on the Dark Web from where they will be able to download the most up-to-date codes, scripts and exploits. In order to obtain such access, a malicious hacker must already have committed certain criminal offenses.

Suicide hackers –this category includes persons who hack computer systems, break services in organisations without a clear goal or plan, do not protect themselves and are easy to trace. The situation in Serbia is that although the number of attacks has increased dramatically in the last 12 years, those who have been involved in unlawful hacking have been at the script kiddie knowledge level, so they were soon discovered. These attacks are mostly misdemeanours, and tracking down such perpetrators is almost certain. In Serbia, the Unit for Countering High-Tech Crime (VTK) deals with this, while simpler cases are solved by the police.

Cyber terrorism –this category deals with cyber attacks with terrorist motives. It does not exclusively involve terrorism, but also the implementation of so-called website defacement with the aim of an attack on a national, racial or religious basis.

State-sponsored hackers –hacking activities performed by hackers who are working for states.[2][3][4] These hackers are actually hired by the state to conduct hacking activities (spying, social engineering, network and computer system penetration, and distribution of malicious programmes) in order to gain advantage over some other country through their access to confidential information. While some sources claim that they are most numerous in Russia, America, and China, and other sources claim that the largest number of state-sponsored hackers is actually in Ukraine,[5] the fact is that this kind of activity is the reality of today. This kind of state sponsorship actually aims to sell its services to other countries. This means that certain states are able to hire out hackers to other countries, in so-called outsource hacking.

2 http://mackenzieinstitute.com/state-sponsored-hacking-mean-canada/

3 https://www.bestvpn.com/state-sponsored-hacking-ukraine/

4 http://www.iss.europa.eu/uploads/media/Alert_5_cyber__hacktors_.pdf

5 http://www.rferl.org/a/ukraine-hacktivist-network-cyberwar-on-kremlin/28091216.html

The unique quality of state-sponsored activities is that the state stands behind them, and this further implies an unlimited budget, and therefore resources as well.

Hacktivism– this term refers to the hacking activities of persons engaged in a particular issue or idea. They are motivated to correct what they think is wrong.[6]Their activities may also include Distributed Denial of Service (DDoS) attacks on terrorist websites, on sites of organisations accused of animal cruelty, on sites of repressive government regimes or on websites of those countries with whose policy they disagree. *Hacktivism* can sometimes be carried out with good intentions, but also provokes collateral damage, causing the innocent to also pay a price. Hacktivists also sometimes help malicious hackers in their pursuit of malicious activities because their motives are not always noble.

Therefore, it can be concluded that malicious activities are determined by the motives, goals and information required for their realisation. When it comes to the motives that lead individuals/organisations to perform a cyber attack, money, power, control, revenge, publicity, the challenge and the testing of security systems are to the fore. The objectives of the attack include attacks on organisations, individuals, states, or political or religious resources.

Since the end of the 1980s, attacks on networks and computer systems have evolved considerably. At first, they ranged from password cracking to external attacks (attacks on poorly configured firewalls, or badly configured isolated networks). By investing in third-generation (so called next-generation) firewalls, organisations have greatly reduced the possibility of an attack from the outside. On the other hand, this has led to the evolution of attack techniques, which have started being run from the inside. An example of this is when there is a malicious insider in the organisation, or when certain social skills are used to deceive the targeted user, who then becomes a malicious insider without being aware of it, i.e., social engineering.

In practice, we no longer need to ask if someone will attack us and whether we can be maliciously hacked, but whether our systems have already been compromised. The key factor is how "interesting" the organisation is for hackers, or when and why it will become interesting. What should be applied in practice is the advice of Eric Cole (a member of the SANS Institute), which has already become a slogan regarding cyber threats: "Prevention is ideal, but detection is a must while its speed is critical."

Security statistics on the basis of appropriate surveys by certain famous statistical companies show that over 80% of organisations have experienced an incident, and what is worrisome is that an attacker (or a malicious programme) can remain unnoticed in large organisations (which have detection and defence systems) for a longer period of time (the cited number is about 205 days in 2014 and 146 days in 2015).[7]

A malicious attack on a computer that has not been updated is extremely easy to perform from a hacker's point of view, and the next step that a malicious attacker performs is privilege escalation to administrator (for example, a user account with user privileges is hacked, and via privilege escalation this account becomes an account with administrator privileges).

Attacks are currently most commonly performed on data, i.e., information, and examples are CryptoLocker ransomware, as well as data destruction (66%).[8]

Also, according to statistics, almost a third of small and medium-sized enterprises (worldwide) have been victims of attacks for no reason other than they are in partnership with some targeted organisations. Most organisations have external

6 https://www.it-klinika.rs/blog/vrste-hakera-i-njihovi-motivi

7 http://files.shareholder.com/downloads/AMDA-254Q5F/0x0x877466/6CADAB40-4539-4DF8-898B-2F58D3E74B51/FEYE_News_2016_2_25_General_Releases.pdf

8 https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

associates from smaller organisations (consulting, marketing, programming organisations). For example, since an attacker cannot hack an organisation that has good protection on its systems (such as a bank), the attack will be shifted to a company that does not pay enough attention to security, and which cooperates with the targeted organisation. The practice has shown that a malicious attacker is waiting for someone from this (unsafe) organisation to make a connection with, for example, a bank (through its Virtual Private Network - VPN) in order to send a previously made document to the bank, which actually contains a malicious payload.

The largest number of attacks come internally by chance (for example, a legitimate employee opens an e-mail attachment or a link and accidentally infects). When malicious content is opened, malicious code (a bot, or a Trojan) is activated, which establishes a connection to the attacker. In practice this means that the connection is made from the inside to the outside, such that the firewall itself and the Intrusion Prevention System/ Intrusion Detection System (IPS/IDS) do not have any special defensive function in that case, because such traffic is mainly allowed. In that case, the defence function that can be applied is a tool that constantly scans sessions and checks at the level of session applications.

According to the Symantec report for 2015, consumer financial losses on a worldwide scale are about $158 billion ($30 billion alone for the US) just for cyber crime, and this data is not complete because a large amount of theft and embezzlement goes unnoticed or unreported, or unpublished and remains unrecorded.

The financial malware known as Tridex has managed to infect over 100 banks and steal about $65million in just 18 months, with a total theft of around $300-350 million. Similarly, so-called crypto mining financial malware targets *crypto currencies,* i.e., it attacks crypto wallets, while blockchain has not been a target of attack.

When it comes to the banking environment, over 80% of attacks come from within the bank itself. The most common targets of attacks are payment cards, comprising as much as 60% of all attacks on banks.

In Serbia, there is financial malware that does not directly target banks, does not deal with attacks on banks, and does not deal with transactions within the banking transaction system, but directly attacks the bank's clients. It is a bot, actually a Trojan, that comes to your computer in various ways: by e-mail, infected USB drives, or it is downloaded from a link, via a torrent, as a crack for a particular programme, etc.... It infiltrates the system and searches an online computer that has certain sessions installed in the form of e-banking connectivity. After finding such a computer, it moves to that computer, waiting for the user to log on to the computer or application, to insert a card and to enter a personal identification number (PIN) code. When all this is done, it activates (in general) a Hyper Text Transfer Protocol (HTTP) injection, i.e., it displays a message on the web page saying "Your transaction is being processed and this will take a while, thank you for *your patience.*" During this time, the background allows an attacker to make unauthorised transactions from that account to certain accounts of financial mules that are used to take illegally acquired money. Financial mules are mainly younger people, typically drug addicts who open accounts for an agreed upon amount but do not know the purpose or background of such transactions. Their task is, upon receipt, to take the money from their account and forward it to a specific person. When the transactions ends, this malware does something or shuts down the operating system (OS) or locks it in order to prevent any checking of the account balance, i.e., to slow down that type of check. It is interesting that this malware exists with a new version that has the ability to wait for a mobile phone (Android type) to be connected via a USB drive and then infects it with the purpose of redirecting calls and SMS texts. In practice, this means the following: at the moment the unlawful activities, i.e., transactions, are carried out, calls

to that number are redirected to some other numbers because banks, in certain cases, check or deal with the control of transactions, and when transactions that were not previously occurring, mainly from legal entities to individuals, happen (that is a trigger) then the banks call the legal entity and request verification. In cases where it cannot be verified the transaction is stopped. However, in cases of redirection to a malicious script, the fake malicious individual would confirm that everything is fine.

One of the biggest compromises of user accounts occurred at the end of 2013 and at the beginning of 2014 and affected 3 billion Yahoo user accounts. Initially, it was thought that 500 million accounts were compromised (names, e-mail addresses, birthdates and phone numbers), but more detailed analysis in 2017 found that this number was actually closer to 3 billion.[9]

In 2014, 145 million eBay user accounts or credentials were compromised.[10][11] It was found that nearly 10 million had recorded account numbers and information with the goal of being able to pay without ever entering payment information. There was a gap between the periods when it was noticed that the accounts were compromised and the moment that users were notified, during which the downloaded data could be abused.

In 2016, in mid-October, hackers compromised 412.2 million accounts of the Adult Friend Finder site. In this way, hackers collected information about names, e-mail addresses and passwords from the previous twenty years from the databases of that site.[12]

At the end of July 2017, data belonging to the Equifax organisation, the largest credit bureau in the USA, was compromised. 143 million items of personal user data such as social security numbers(SSNs), dates of birth, addresses, and even drivers license numbers were compromised, and 209,000 users' credit cards numbers were compromised.

In 2018 the data of 150 million MyFitnessPal user accounts of the UnderArmour organisation was compromised. There are indications that data such as names, e-mails and hashcode (password verification) values was compromised.[13][14]

In 2018, data from almost 50 million user accounts of Facebook was compromised[15] which is one of the biggest security failures in Facebook's history. Malicious attackers stole "access tokens", which represent a kind of security key that allows users to stay logged on to Facebook during simultaneous web sessions without the need to re-enter their login information. The possession of "access tokens" allows the malicious attacker to take full control of the victim's account, even including the possibility of logging in through third-party applications used for logging in on Facebook.[16]

A troublesome fact is that the increase in the total amount of malware on the Internet since 2009 has been drastic. The total number of malware instances in 2009 was 29.48 million, and in 2018 it has so far amounted to 836.97 million.[17] Compared to 2017, the total number of malware instances has increased by 117 million. This means that in the past year, 9.75 million malware instances occurred every month, or about 325,000

9 https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

10 https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/

11 https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

12 https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

13 https://www.thesslstore.com/blog/2018-cyber-crime-statistics/

14 https://www.cnbc.com/2018/03/29/under-armour-stock-falls-after-company-admits-data-breach.html

15 https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach

16 https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach

17 https://www.av-test.org/en/statistics/malware/

new malwares are detected every day.[18] As such, it can be concluded that every day worldwide, a large number of people are engaged just in the production of malware.

Vulnerability or the possibility of infection occurs when the system or application is not patched, i.e., updated. If a computer system connects to the Internet without the latest security patches, regardless of antivirus efficiency, there is a real chance that in less than 20 seconds the computer will get infected. This is possible because in practice it is feasible to use an exploit over 5 years old, recognised by all antivirus or antimalware programmes, but encrypted by certain tools so that it gets a "capsule" around it and becomes "invisible" and, therefore, is not detected by most antivirus programmes (there are free antivirus engines that check the maliciousness of files with the most common antivirus solutions online). It is alarming that a large number of small companies do not make updates or that updates are only performed once every 3-6 months. This means that when a zero-day appears, the patch for it is published in one month on average, and if the system is updated only once in six months, from a security perspective, the update does not work at all.

Attacks are never random, they are always targeted and mostly paid in advance, as experience has shown that criminals are organised into groups as companies. Hacktool Multipurpose, which appeared in 2015, and was present near the end of 2016 (though it can no longer be found on the regular Internet but it can be found on the dark web) served to create malicious programmes where, in a very simple way, malicious functions can be visually programmed and include a shield, and where as output, a personally written malware is obtained. The thesis that high-tech criminals are organised into groups and operate as organisations is supported by the fact that this tool also had support for obtaining answers to problems related to the use of the tool. Also, new malware and ransomware have their own support. In practice, in the event of infection, ransomware files are encrypted and information regarding the amount of money that should be paid, as well as the entire procedure, is received, and there is an active call centre with an operator providing information on payment options. After analysis of Trojan activity, such as that completed by FireEye labs[19] on Dridex,[20] one of the pioneers in financial malware, it appears that these malicious activities have their working and non-working days where activities are suspended during holidays. Therefore, there are companies dealing with malicious activities, that keep regular business hours. This thesis is supported by the fact that the platform Cybercrime-as-a-Service is mentioned more frequently. In 2018, one of the world's largest DDoS renting services "webstressor.org" was closed. This site had over 136,000 registered users. The services of this organisation could be used by users with little or no technical knowledge to launch a DDoS attack for about £10. The services of this organisation were responsible for the attack not only on the seven largest banks in Great Britain in 2017, but also on some state institutions and gaming services.[21]

In one statistic, data on the indicative amounts offered by the "Cybercrime-as-a-Service" platform is provided.

RECOGNIZING AN ATTACKER'S STEPS USING DIGITAL FORENSICS

In most cases, the first step in the planning of malicious attacks is the formation of a malicious programme, followed by reconnaissance in terms of finding a target, collecting data, scanning,

18 These are not zero-day malware, but derivatives.

19 https://www.fireeye.com/blog/threat-research/2016/01/dridex_botnet_resume.html

20 https://www.symantec.com/connect/blogs/dridex-financial-trojan-aggressively-spread-millions-spam-emails-each-day

21 https://www.thesslstore.com/blog/2018-cybercrime-statistics/

Cybercrime Product or Service	Price (in US Dollars)
SMS Spoofing	$20/month
Custom Spyware	$200
Hacker-for-Hire	$200+
Malware Exploit Kit	$200-$700
Blackhole Exploit Kit	$700/month or $1,500/year
Zero-Day Adobe Exploit	$30,000
Zero-Day iOS Exploit	$250,000

Source: https://www.thesslstore.com/blog/2018-cybercrime-statistics/

hacking, eavesdropping and exploiting the system through malicious software. A characteristic of most malicious attacks is enabling re-entry of a malicious attacker into the system and erasing any traces.

Creating malware - it can be said that the starting point for creating malware starts with open source applications, because the source code is open and the attacker can download and review it and then conclude with analysis of where the weaknesses of that code are. Lately, fileless malware, i.e., malware that does not have a file or payload and does not stay on machines other than in the registry, stays mostly in memory and lasts while the computer is turned on. Fileless malware is very difficult to recognise, sandbox security testing areas does not recognise it and it is increasingly in use. According to some statistics, almost a quarter of the world's malware is comprised of this type. For example, some interesting malware of this type searches to see if there is a PowerShell on a machine, sends the PowerShell a command, creates a script directly into PowerShell on the victim's computer that is connected to the Internet and loads it into memory.[22] It has the same form as any other malware, but this is a new technique in the sense that it is detected by almost no antivirus. Also, SMS malware is a novelty –an example of which is a message of the Nigerian scam type with a link where the offered reward is received by SMS, but actually clicking the link leads to a malicious server.

After creating the malware, the next phase is the reconnaissance phase, i.e., finding and scanning the target and obtaining information about whether there is specific software/service on the server that has a certain weakness. Scanning of the OS itself is one of the first steps which a malicious attacker performs in order to determine the operating system, which open ports it has, which protocols are missing, etc. The term footprinting, besides scanning of the OS, can also include determining the type of business of an organisation, how many people are permanently employed in it, their profiles, etc. Therefore, reconnaissance is observation that involves collecting information about the organisation or the individual who is the target of the attacker. It can be active and passive. Active observation is a direct scan of the target, for example, the use of tools that directly send packets to the targeted system to find out more information about it (one of the tools is a trace route used by attackers to find out the router's IP addresses or firewalls protecting the target). Hence, an active observation involves the scanning of ports and the OS. Passive observation means the collection of data without direct contact with the target (searching of social networks and sites that carry information about the target). Logical and technical approaches for finding the target and collecting data about it are more in use, rather than the former physical modes (tracking a

22 http://thehackernews.com/2017/02/fileless-malware-bank.html

potential target by physical surveillance). Nowadays, with Internet technology it is much easier for malicious attackers to track a potential target by using social networks to track users. For example, there are a lot of people who, due to their need to show off brag about luxuries they possess, provide information on social networks about where and when they are travelling and when they are returning from a trip. Most users are not even aware that in this way they actually provide data about their whereabouts and facilitate the job for the attackers, tipping them off as to when they are not at home. Also, attackers use social engineering methods to get as much data on the target as possible. For example, an attacker can collect data from business social networks (for example, LinkedIn) about a portfolio of specific user professions (users leave information about where they have worked, where they are working now, and on what jobs). In the case that some organisation offers employment for security administrators, the attacker can find people who worked or who are working now in that organisation with the help of LinkedIn and, through their profile, learn which services a particular organisation has implemented in their network environment. Additionally, passive observation includes listening to regular traffic in order to obtain information about possibilities and vulnerabilities when it comes to a server as a target. Passive observation generally begins with searching for information in the Domain Name System (DNS) and the Whois database. In cases where a domain in which the target system is registered is known, the attackers usually use commands such as nslookup, dig, and whois in order to obtain as much target information as possible.[23]

In forensic practice, a typical scenario of attackers' further steps is noticeable. After using active and passive hacking techniques that are often used to find a specific target of attack (IP address and exact location of the attack), the next step of the attacker is to scan vulnerabilities on the target. In addition to the attacker receiving information about open ports, missing protocols, and operating system version (with some tools it is possible to get information about the last installed patches), information on the vulnerabilities that are available on that system will also be obtained. *The attacker's next step is to actualize the attack, gaining access to the system by hacking in via the release of a particular exploit that abuses a found vulnerability. When attackers gain access and escalate privileges, they usually set up a persistent backdoor or maintain access malware mechanism. This means that in the event of a computer shutdown or restart, a malicious attacker can re-establish the connection to the system (in fact, a compromised computer establishes a connection to the attacker's system). In the end, the attacker will attempt to clear all traces, because traces of whatever happens on the OS are left in logs. Based on logs, it is possible to do a backtrace and on the basis of forensic analysis it is possible to identify the perpetrator of illegal activity. Since attackers try to erase log files while attempting to erase traces, it is recommended that logging take place on special log servers, as this would prevent attackers from deleting the files. In large organisations, there are usually Security Information and Event Management (SIEM) solutions or log management systems that collect logs, so an attacker can erase logs, but these logs have already been forwarded to log management. It is vital to note that it is extremely important to carefully configure the synchronisation of logs with log management. If the synchronisation time is poorly defined an attacker can use that delay, and in that period if an attacker makes a malicious script that deletes logs on a local computer in that "defined synchronisation time," the log will never reach log management and the alarm will not be activated.*

In the past couple of years, classic system hacking techniques that use classic exploitation of some vulnerability that exists on a system have returned to the field of cyber crime. As defence tech-

23 http://itsecurity.telelink.com/reconnaissance/

niques evolve, the accent is on updating mostly newer techniques, and old ones protecting certain vulnerabilities have remained without updates.

A malicious attacker is always motivated by a certain routine, knows the attack method and knows the vulnerability to abuse. When it comes to motive, money is primary, followed by terrorism, politics, or competition. The method involves the techniques and tools that a malicious attacker uses to abuse the system. Vulnerability can be logical in the sense of an unpatched or poorly configured system (poor configuration of access control).[24] Uninformed workers or users in an organisation are also considered vulnerabilities, due to poor knowledge of information security. This may be an even bigger problem than poorly configured or unpatched systems. It is therefore important that the organisation recognises the importance of security awareness training.

The most commonly used methods used by malicious attackers when it comes to networks are sniffing, spoofing, *Man*-in-the-*Middle* (MiTM) attacks, poisoning attacks, attacks on passwords (easy cracking of poor passwords), Denial of Service (DoS) attacks and attacks on devices used for defence (firewalls, IDS). Sniffing means eavesdropping. Spoofing is lying, i.e., a falsely represented identity. MiTM involves eavesdropping on the basis of insertion between two sides in communication and intercepting all traffic. MiTM is extremely dangerous, since apart from interception it allows changes to the traffic itself. In addition to the MiTM at the Hyper Text Transfer Protocol (HTTP) level, it can also be performed at the HTTP Secure (HTTPS) level. Unique to HTTPS is that it cannot be eavesdropped,[25] but a malicious attacker, by stealing cookies, can falsely present and make a session to a particular server as a legitimate user. Poisoning, as a forerunner of spoofing, is a method by which cache "poisoning" on switches and routers is possible, with the aim of redirecting traffic to and from a malicious attacker. The target of poisoning is, in the first place, the DNS in order to direct the traffic of legitimate users to a malicious site which has been prepared in advance. For example, instead of users going to a Twitter site, the user will be redirected to a false Twitter site prepared by a malicious attacker in order to collect credentials from a particular victim. Attacks on passwords involve the extraction of hashes, from which the password will be reproduced. DoS, i.e., denial of service (and its derivatives of Distributed DoS, i.e., DDoS, and Reflected Distributed DoS, i.e., RDDoS), means the disabling of particular services by directing vast amounts of traffic to a victim.

Another type of malicious attack refers to host attacks through certain malicious applications. In this case, the aim of the criminal attacker is to gain unauthorised access to the particular system and escalate privileges to the administrative level. Also, backdoors (Trojans) are used to ensure renewed access to the compromised system. Hardware or software keyloggers (programmes that capture keystrokes) are extremely dangerous (since they are rather undetectable) especially when organisations have the ability to implement them on a legitimate level in terms of supervision, as a form of protection of their own systems, with which the employee has been acquainted when signing a contract, although this is contrary to privacy rights.

Fig. 1 CIA Triad

24 https://www.netsparker.com/blog/web-security/logical-vs-technical-web-application-vulnerabilities/

25 SSL can legitimately be "eavesdropped" at the level of the organisation if on the so-called "wiretap" device certificates for encryption and decryption are imported.

The CIA Triad as a basis of IT security and layered protection (defence in depth)

Confidentiality – no one can reach the information except the person for whom this information is intended.

Integrity – the information itself is protected and cannot be changed.

Availability –the service is available to the person for whom it is intended at the moment it is needed.

The challenge of protecting information is to find a good balance between safety and functionality.

If something is confidential, and its integrity is protected, but not available to whom it should be available, then it is useless, while if it is available, but not safe then it is not secure. Therefore, it is necessary that all three conditions are met in order to have quality in security, but it is necessary to find the optimal balance in order not to endanger the functioning of the organisation.

As an addition to the CIA model, 3 additional measures are as follows:

Authentication –checking or identifying the user,

Access control,

Non-repudiation.

In order that a user has access to a particular file that is part of the CIA system, a user name and password are necessary, i.e., authentication is required. Access control is also required (in the sense of up to which levels the logged user can have access and what can be accessed), as well as non-repudiation, i.e., something that is appropriate actually to accountability or logging, where the trace of who had access and what has been done is visible, such that in case some problem occurs later on, it will be possible to claim with non-repudiation that a specific person did something.

Additionally, attention must be paid at all levels to security problems in order to have complete and adequate protection. The layers referred to in the Open Systems Interconnection (OSI) model range from the physical layer (wires) through the transport layer to the application layer.

At the physical layer, the starting point is that everything, all devices and all wires, can be intercepted. Data transfer methods can be intercepted, for example, in the way that if copper wire is used for data transmission malicious attackers can use vampire taps for eavesdropping (in this "clamping" procedure attackers actually create a bridge towards themselves in order to intercept communication). If unshielded twisted pair (UTP) cable is used as a physical medium, there are also vampire taps for UTP, but this is hardly feasible, since each UTP wire must be clamped individually. Generally, attackers use a transmission sniffer signal wrapping the UTP cable with the aim of eavesdropping on everything that goes through it. The defence procedure is to additionally shield a cable, i.e., to have the wires go through metal shields when they go through the wall.

At the transport layer, malicious attackers can eaves drop using software or logical methods. It is, therefore, important to implement protection on the network according to IPSec security protocol principles and via session check-ins. It is very important that when sessions are started on a server, certain security algorithms for forming session IDs are applied to the server, because the malicious attackers try to reproduce session IDs for session hijacking that is to steal the session.

At the application layer, implementation of applicative filters and applicative control over application activities is necessary. Modern protection systems have session-level controls, which means that every communication from an organisation to the outside or inside includes a check of what is being done and what is being accessed, and on the basis of different signatures it can be detected whether or not communication is normal, with the session interrupted accordingly.

CONCLUSION

In addition to providing physical security, it is necessary to set up appropriate teams for incident management and vulnerability management on critical systems and to define a time period for penetration testing. In this way the system security checking will be carried out externally. In addition to legal regulations and acts, and in order to ensure protection at all levels, organisations must use their own security procedures. Enterprise Information Security Architecture (EISA) is a standard that can help to determine the measures that have to be undertaken in order to provide security at the highest possible level. Safety policies or documentation with procedures and instructions relating to safety must be available to everyone in the organisation. In addition to all the listed methods of protection, one should always keep in mind that the weakest link in the protection system is actually the human factor. The method of obtaining sensitive (i.e., cryptographic) data by using a person who has knowledge of that data is called social engineering (Hadnagy 2011). Each individual should have a security culture, a so-called security awareness within the environment in which this person works (home or office). The purpose of security awareness is that every individual must consider that the security of the organisation also depends on his individual responsibilities (Nadeem 2018). Besides using defence tools, multiple security systems, and cryptographic mechanisms, educating people in security awareness is crucial and is one of the security factors that must be continuously implemented.

* * *

BIBLIOGRAPHY

Hadnagy, Ch. 2011
Social Engineering: The Art of Human Hacking, Indianapolis: Wiley Publishing.

Lanier, C. 2018
The Types of Hackers & Why They Hack, Bleeping computer, https://www.bleepingcomputer.com/news/security/the-types-of-hackers-and-why-they-hack/

Nadeem, M. S.
Social Engineering: What is baiting?
https://blog.mailfence.com/what-is-baiting-in-social-engineering/ (June 30th 2018).

REZIME

TARGETIRANJE SAJBER PRETNJI NA OSNOVU PREPOZNATIH ZLONAMERNIH AKTIVNIH I PASIVNIH TEHNIKA NAPADA I ZAŠTITA INFORMACIJA

KLJUČNE REČI: SAJBER PRETNJE, ZAŠTITA SISTEMA, ZAŠTITA OD NAPADA.

U ovom radu su opisane tehnike napada prepoznate u digitalnoj forenzičkoj praksi kojima se služe zlonamerni napadačida da bi izvršili upad u sistem. Razgraničen je pojam hakera i zlonamernog napadača u zavisnosti od ciljeva i motiva kojima su vođeni. Prikazani su neki od najvećih sigurnosnih propusta velikih organizacija u poslednjih 5 godina i njihova šteta u pogledu kom-

promitovanih korisničkih kredencijala. Dato je pojašnjenje u vezi sa CIA trojstvom kao osnovom IT bezbednosti zajedno sa dopunskim merama i slojevitom zaštitom. Cilj ovog rada je podizanje bezbednosne svesti kako kod korisnika koji rade u svojim organizacijama u internet okruženju tako i kod pojedinaca koji su home based orijentisani. Pored korišćenja alata za odbranu, višestrukih sistema zaštite, i upotrebi kriptografskih mehanizama, edukacija ljudi po pitanju security awerness-a je ključna i jedna od faktora bezbednosti koji mora kontinuirano da se sprovodi.