Zoran Cekerevac - Zdenek Dvorak - Ludmila Prigoda - Petar Cekerevac*

HACKING, PROTECTION AND THE CONSEQUENCES OF HACKING

Understanding the term hacking as any unconventional way of interacting with some system it is easy to conclude that there are enormous number of people who hacked or tried to hack someone or something. The article, as result of author research, analyses hacking from different points of view, including hacker's point of view as well as the defender's point of view. Here are discussed questions like: Who are the hackers? Why do people hack? Law aspects of hacking, as well as some economic issues connected with hacking. At the end, some questions about victim protection are discussed together with the weakness that hackers can use for their own protection. The aim of the article is to make readers familiar with the possible risks of hacker's attacks on the mobile phones and on possible attacks in the announced flood of the internet of things (next IoT) devices.

Keywords: *hacking, hacker, information technology, internet of things, protection, economics*

1. Introduction

Under a term, the hacking one can include any unconventional way of interacting with systems, i.e. interaction in the way that was not foreseen as a standard by the designer, [1].This term is mainly connected with the modern technologies hacking, computers and computerized devices. So, the computer hacking is broadly defined as intentionally accessesing a computer without authorization or with exceeding of authorized access. More detailed about the legal aspect of hacking is given in [2], [3], [4], [5]. In any case, and above all, the hacker is responsible for the legal consequences of his actions.

What is considered by unconventional interaction with the system? The document in MS Windows can be opened in various conventional ways, one of which is double-click on the icon of the document, or, the second, double click on MS Word or Excel, and then the opening of one of the memorized files, etc. There are also other ways of opening documents using MS Office, or Open office, but they are considered as conventional. The same document can be accessed in any other way, for example, from another operating system, completely bypassing Windows and office software, and reaching the document in the text format. Such a method is considered as unconventional. And whoever accessed the document in this way can be called a hacker.

2. Who are the hackers?

The hacker can be anyone if he/she has a basic knowledge, desire, motivation, and (sometimes) some money. In addition to these characteristics, the successful hacker must have a large dose of patience and planning workability. However, neither all hackers are all the same, nor all hackers have the same goals. They are usually categorized into three main groups:

1. Black-hat hackers
2. White-hat hackers and
3. Gray-hat hackers.

Per relevant information sources, "a black hat hacker is a person who attempts to find computer security vulnerabilities and exploit them for personal financial gain or other malicious reasons" [6]. So, the Black-hat hackers are bad guys. Per the same source, "a white-hat hacker is a computer security specialist who breaks into protected systems and networks to test and assess their security. The White-hat hackers use their skills to improve security by exposing vulnerabilities before malicious hackers (known as black hat hackers) can detect and exploit them." But, the world of hackers is not black and white. There is also the third big group, the Gray-hat hackers. "A gray-hat hacker is someone who may violate ethical standards or principles, but without the

* [1]**Zoran Cekerevac**, [2]**Zdenek Dvorak**, [3]**Ludmila Prigoda**, [4]**Petar Cekerevac**
[1]Faculty of Business and Industrial Management, "Union - Nikola Tesla" University in Belgrade, Serbia
[2]Faculty of Security Engineering, University of Zilina, Slovakia
[3]Faculty of Economics and Service, Maykop State Technological University, Maykop, Russia
[4]Hilltop Strategic Services, Belgrade, Serbia
E-mail: zoran@cekerevac.eu

https://doi.org/10.26552/com.C.2018.2.83-87

malicious intent ascribed to black hat hackers" [6]. The Gray hat hackers are often operating for the common good.

In practice, in communications, a term: "Ethical hacker" can also be heard, but discussion about ethics can be a wide and slippery terrain. Is it ethical to spy own children "for their good"? So, we'll stay in the named group. It is interesting that all of them use the same tools and methods, and the main difference is in their aims and results. On the other hand, hackers can be divided into several groups according to their knowledge and skills. The highest level consists of hackers who know exactly what they do, that are very familiar with the system and are able to create the appropriate software, including viruses and another malware. The middle level consists of the so-called "technicians" who are able to use tools that can be purchased in the market of software and hardware. The third, the lowest level of hackers, consists of the so-called "script kiddies". A script kiddie is a derogative term for the more immature, but unfortunately often just as dangerous exploiter of security lapses on the Internet. They exploit weaknesses in the Internet computers often randomly and with little regard or perhaps even understanding of the potentially harmful consequences [7].

3. Why do people hack?

Hacking can be done for different reasons. However, the following four groups can be distinguished:

- One of the first reasons is collecting data. In doing so, the data can be very varied, from business data to the private data, practically anything and everything, from important to useless.
- Another group could be the impersonalization of persons or clients. Thereby, there can be collected numbers of bank accounts, e-mails, and the like. One of the reasons for the impersonalization can be preparing for a distributed denial of service (next DDoS) attack.
- The third reason can be of destructive nature. The targets of destruction may be websites, databases and the like. The main objective, in this case, is to make damage.
- The last, but very often reason for hacking is hacking for fun. Many find a pleasure in burglary into other people's systems, walk through them and come out unnoticed. Will they, in fact, have some benefit, (if they even have) is the less important for them. Any significant inroads into the specific network, like Pentagon, Central Intelligence Agency (next CIA), etc. increase their dose of adrenaline.

4. Hacking and the law

The Internet, as a rather modern technology, brings new challenges. It is very difficult to define what is right and what is wrong. If some user publishes his email address, and the other involve this address in its database and sends a bulk of emails to this address, is it legally or not? Privacy and the information privacy are a great issue. The person or institution, who owns the computer, or the computer system is not necessarily the owner of the data on that system. Internet service providers that host Web sites are not the owners of the contents of the hosted websites. The doctor who owns a database on their patients is not the owner of those data and if he publishes them he can found himself in a big trouble.

5. Methods of hacking

Data can be stolen in a variety of ways, from the brutal theft of the entire computer, over the copying of contents of hard drives, to sophisticated methods by remote access.

The easiest way is to steal data from the inside. It can do permanent employees dissatisfied with working conditions, temporary or part-time employees, or even an employee in charge of security and maintenance of the system. Access can be provided through the so-called backdoor. If he provides a constant external connection and on cable glues a label "Security - Do not unplug" it is likely that no one will with interfere this connection until the new reconfiguration of the system. In all these actions a direct physical contact with the device is necessary.

The attacks carried out on the network are more sophisticated and usually include searching for an open access port, email addresses and passwords, DDoS, access to file servers, holes in the firewall, etc. One possibility is the use of backdoors that many manufacturers left open for the purposes of control of the products.

The development of software and hardware can be a quite boring job. These activities require frequent testing, resetting, connecting different contacts and/or parts of programs, troubleshooting and the like. If any change would require re-authentication, this would significantly reduce the work efficiency. Therefore, developers initially leave open the possibility of applying various, only to them known, commands that skip certain phases of work. They are called "Easter eggs". As a rule, those controls should be deleted from the program code as work is completed. However, very often, the Easter eggs remain permanently in the software. By testing different key combinations, or by user error, or accidentally, users can find and use them. As an example, keyboard shortcuts for Microsoft Word on Windows can be used [8].

For realization of the hacking, it is unavoidable to use the social engineering. There is a variety of diverse and imaginative solutions, but one of the stupidest and the most frequently applied, is that by an e-mail, the attacker from their victim requests to provide personal information, including the password for the specified e-mail address, so as not to be ruled out in the next few days. It is needless to say about the possibilities that attacker gains using these data. This hack is based on sending mass e-mails. One of the frequently used is the variant in which some person is aimed to be a victim. E.g. an attacker, using a disposable cell phone, calls on the victim posing as a representative of the Internet service provider or bank in which the victim has an account. The attacker explains to the victim that there is some problem with a victim's account that the operator cannot solve without the help of the victim and that he needed a password for that purpose. Surprised victim usually tells their password. Fraud can continue by the offering of providing help for payment of outstanding bill if the victim provides the credit card information, etc.

In addition, phishing, fake emails and fake websites are used in hacking, but they will not be discussed here.

6. Planning of attacks

Hacking is the real threat of today's virtual world. There is no attack that can be realized by pressing a single button with just passing by the computer or mobile phone. Even when a hacker has access to a victim's computer within a reasonable time (which is never the case) and when "only" needs to find a password for email or logging in, it might be mission impossible. Such attempts were unsuccessful and quickly point to the perpetrator.

From the aspect of an attacker, as well as from the aspect of a defender, there are several things that need to be considered:

- What does an attacker want to achieve using the attack?
- What can be profitable to an attacker? Stealing of banking credentials might not be profitable. This hack can be solved in a few minutes, by only one telephone call. For an attacker, it is more favorable, and for the victim more dangerous, if the attacker takes over credentials of PayPal, E-Bay, amazon.com, a directory of users, etc. If the attacker is a parent, what he/she wants to follow?
- The next question is: How to realize the attack? Among many possibilities, there are two main approaches:
  - a mass attack that demands long and careful planning and preparation, and adequate malware and
  - a targeted attack that demands careful analysis and collecting data about a concrete person or a company.
- The final question for an attacker and for the defender is: Which information the attacker wish to get?

From the attacker's side, there is also a question concerning the available tools.

And finally, and perhaps it is better to put it at the very beginning, there is a question about the profitability of the action: what will happen in the most favorable case, and what in the most unfavorable case?

7. Economic aspects of hacking

Quantifying losses caused by the cyber-attacks is very difficult and unprecise. Losses consist not only of the direct cost of lost money, but of the costs of cleaning up and the investigation, as well. In addition, every day improving protection costs money. And information technology staff do not work for free. The year 2011 was called "The Year of the Hack" [9]. According to that source, hackers earned 12.5 billion USD that year. A lot of companies did not publish their financial losses, but among the companies that did it there are:

- Sony, with 171 million USD;
- Citigroup, with 2.7 million USD;
- Stratfor and AT&T, with 2 million USD each; and
- Fidelity Investments, Scottrade, E*Trade, Charles Schwab, with 1 million USD.

Per Richard Power, from the Computer Security Institute, "single instances of hacking may cost as much as $600,000 to $7 m a day for online businesses in 2011, depending upon the revenue of the operation" [10]

Author of [11] stated that the hackers cost U.S. economy up to 500,000 jobs each year. In his study, he blames the Chinese hackers for espionage. This analysis was based on similar reports of McAfee and the Center for strategic and international studies [12]. The authors of the study said that each time when an information is stolen, some company went into the risk of bankruptcy. They estimate that hacking costs the US economy up to USD 100 billion a year.

Hacking reached enormous sizes, and each year it getting bigger and bigger. The Chinese side is constantly accused for espionage and eavesdropping. Such an analysis is given in [13]. On the other hand, a book was written about the computer virus Stuxnet that was designed by the USA and Israeli computer experts to sabotage the Iranian nuclear program [14]. This was the first known cyber weapons used in the war with the aim of destroying the infrastructure of a country. Finding of the Stuxnet malware successors Duqu and Duqu 2.0 suggests that the arms race was never interrupted and that in parallel with conventional forms cyber warfare exists. Many articles were written about other examples of hacking and cyber espionage, like projects PRISM and Tempora [15], [16], [17], [18], [19], [20], so those will not be further discussed here.

8. Attacker's protection

In any case, a hacker needs to think about self-protection. All Internet activities can be, and they are, monitored and tracked via Internet service provider (next ISP), network routers, a computer system. Although this is happening 24/7, the collected data are rarely used. Only if the attackers caused serious problem he could expect legal consequences.

Each hacker intends to work remotely from a place, which is far away from his home. In addition, the attackers change their location frequently choosing locations and computers that cannot be easily connected with them. For conducting an attack the best for attackers is the use of others computers, for example, computers in public libraries, cafes, or, eventually, cheap computers that can be destroyed immediately after use. One possibility is the use of operating systems and software written on CDs on computers from which the HD was previously removed.

That hacking is risky tell the fact that all financial transactions a hacker needs to make with money in cash. The alternative can be using pre-paid credit cards and telephone numbers.

9. Victim's protection

On the other hand, a defender needs to know the way of an attacker thinking and methodology, as well as about the tools, which attacker can use. An organization can suffer a lot from a hacker attacks. When the organization survives an attack, it needs to make deep changes it its protection, must apply a new philosophy, very often with the new staff. Some organizations outsource their protection. So, many new independent companies can benefit from specializing in hacking prevention. Outsourcing can be a good solution for small and medium companies because of their limited staff and money capabilities, [21], [22], [23].

10. Conclusions

To protect a computer and/or a computer system from hacker attacks, a defender needs to know the way of an attacker thinking and methodology, as well as about the tools, which attacker can use.

All attackers use similar methods and tools. Their intentions can determine whether they will be the Black-hat, Gray-hat or White-hat hackers. A hacker attack needs time, and cannot be realized without a lot of work.

According to the latest research, majority of users do not recognize attacks at all, some of them identify attack within 200 days and only a few manage to identify and react on attack within 24 hours. If the attack on informational system does not corrupt data, the chance that system administrator will identify an attack is very low. If the data was corrupted, the chance for recognizing of an attack is rising.

The authors of this paper in no case encourage readers to engage in risky hacking especially of the Black-hat hacking type, but they want to make readers familiar with the possible risks in the announced flood of the IoT devices.

References

[1] Eli the Computer Guy. Introduction to Hacking [online]. Available: https://www.youtube.com/watch?v=yGIHjTmTFfA [accessed: 2010-12-12].

[2] JARRET, H. M., BAILIE, M. W.: Prosecuting Computer Crimes [online]. Available: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.

[3] National Assembly of the Republic of Serbia. Law on Organization and Jurisdiction of State Authorities for Combating High-Tech Crime [online]. Available: http://www.paragraf.rs/propisi/zakon_o_organizaciji_i_nadleznosti_drzavnih_ organa_za_borbu_protiv_visokotehnoloskog_kriminala.html [accessed: 2017-03-18].

[4] Ukrainian National Assembly. Law of Ukraine of 7 September 2005 ℓ 2824-IV on the Ratification of the Convention on Cybercrime (with amendments and addenda of 2010-09-21) [online]. Available: http://search.ligazakon.ua/l_doc2.nsf/link1/T052824.html.

[5] Kazakhstan. Proposed a Convention Project to Combat Cyberspace [online]. Available: http://www.zakon.kz/4808903-rf-predpolozhila-proekt-konvencii-po.html [accessed: 2016-08-01].

[6] Black Hat. Black Hat Hacker [online]. Available: http://www.blackhat.com.

[7] ROUSE, M.: Script Kiddy [online]. Available: http://searchmidmarketsecurity.techtarget.com/definition/script-kiddy.

[8] Microsoft. Keyboard Shortcuts for Microsoft Word on Windows [online]. Available: https://support.office.com/en-us/article/Keyboard-shortcuts-for-Microsoft-Word-on-Windows-95EF89DD-7142-4B50-AFB2-F762F663CEB2.

[9] STANESCU, B.: Top 5: Corporate Losses Due to Hacking [online]. Available: https://hotforsecurity.bitdefender.com/blog/top-5-corporate-losses-due-to-hacking-1820.html.

[10] GISH, W.: The Effects of Computer Hacking on an Organization [online]. Available: http://smallbusiness.chron.com/effects-computer-hacking-organization-17975.html.

[11] LEWIS, J. A.: Economic Impact of Cybercrime [online]. Available: https://www.csis.org/analysis/economic-impact-cybercrime.

[12] SMITH, G.: Hackers Cost U.S. Economy Up To 500,000 Jobs Each Year. Study Finds [online]. Available: http://www.huffingtonpost.com/2013/ 07/25/hackers-jobs_n_3652893.html.

[13] BARRET, D., YARDON, D., PALLETA, D.: U.S. Suspects Hackers in China Breached about 4 Million People's Records. Officials Say [online]. Available: https://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888.

[14] SANGER, D. Obama Order Sped up Wave of Cyberattacks against Iran [online]. Available: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyber attacks-against-iran.html?_r=3&adxnnl=1&pagewanted=all&adxnnlx=1338548715-2wt62+m6D3KzuVRTaa2QJQ.

[15] DERESPINA, C.: WikiLeaks Releases 'Entire Hacking Capacity of the CIA'WikiLeaks Releases 'Entire Hacking Capacity of the CIA' [online]. Available: http://www.foxnews.com/us/2017/03/07/wikileaks-releases-entire-hacking-capa city-cia.html.

[16] BACON, J.: WikiLeaks: CIA Can Hack into Phones, TVs-Everything [online]. Available: http://www.usatoday.com/story/news/nation/ 2017/03/07/wikileaks-says-has-published-cia-hacking-codes/98844256/ [accessed: 2017-03-07].

[17] SCEKIC, D., CEKEREVAC, Z.: Privacy by Design - Possible Solution in the Protection of Privacy and Personal Data. Proceedings of International Scientific-Professional conference Information Technologies, Economics and Law: state and development perspectives (ITEL-2016), USA, 260-262, 2016.

[18] JASEK, R.: SHA-1 and MD5 Cryptographic Hash Functions: Security Overwiev. Communications - Scientific Letters of the University of Zilina, 17(1), 73 – 80, 2015.

[19] CEKEREVAC, Z., DVORAK, Z., CEKEREVAC, P.: Internet Safety of SMEs and E-mail Protection in the Light of Recent Revelations about Espionage of Internet Communication System. Zbirnyk naukovykh prats Bukovynskoho universytetu, Ekonomichni nauky, 10, 25-33, 2014.

[20] KUBINA, M. & KOMAN, G.: (2016). Big Data Technology and its Importance for Decision-Making in Enterprises. Communications - Scientific Letters of the University of Zilina, 18(4), 129 – 133, 2016.

[21] PRIGODA, L., CEKEREVAC, Z., DVORAK, Z., CEKEREVAC, P.: One Look at the Modern Information Security [online]. Sustainable Development of Mountain Territories, 4(22). Available: http://www.meste.org/cekerevac.eu/biblioteka/ij_23.pdf.

[22] CEKEREVAC, Z., CEKEREVAC, P., VASILJEVIC, J.: Internet Security of SMEs is an Aspect of Security E-mail. FBIM Transactions, 2(1), 45-56, 2015. DOI:10.12709/fbim.02.02.01.05

[23] CEKEREVAC, Z., RADONJIC, S.: Some SMEs Data Safety and Security Issues in the In-House and in the Cloud Computing. Proceedings of 18th International Science Conference Solving of Crisis Situations in a Specific Environment, Slovakia, 99-106, 2013.