Survey on Hacking Analysis and Mitigation Techniques

Ricardo Neves

University Lusófona of Porto
Porto, Portugal
ricardomanuelvalenteneves@gmail.com

Abstract. Year by year, technology has evolved and integrated itself into our lives, allowing us to explore a new world where we can access or share relatively anything we want. Consequently, in today's society, we are present with constant use of those technologies and thus an accompanying and permanent flow of data throughout the world. This information, available on the internet, appears in various forms, such as images or texts, and holds its value. Therefore there will be entities that will try to obtain this data for numerous purposes with mixed approaches. Specifically, cyberattacks have been a common threat to both the data and the users of the internet. One of the most popular and common cyber threats is known as malware. This malicious software finds its way to our devices through various ways with different objectives, having only in common its intent, which is to damage computer systems. This survey will cover hacking analysis by deconstructing cyberattacks throughout its chapters and providing a practical application on a malware analysis, bringing forward a deeper understanding of hacking and mitigation techniques.

Keywords: Cybersecurity, Cyberattacks, Hacking Analysis, Mitigation Techniques, Network, Cybercrime, Hash, Strings, Cyberspace

1 Introduction

Currently, cybersecurity is a broad field that follows the ongoing growth of modern technology [1]. Acknowledged as one of the most notable drawbacks to governments, corporations, and individuals in the current century [2], cybersecurity plays a significant role in the lives of those who interact with cyberspace. Moreover, it extends through multiple sectors with various media articles and studies showcasing the harm caused by hacks to the respective, be it healthcare [3] [4], economics [5], or others.

The Federal Bureau of Investigation, commonly referred to as the FBI, is a well-known justice department whose actions have significantly benefit the victims of cybercrimes. Furthermore, it is also an exceptional source to understand the necessity of cybersecurity, mainly due to their publications in regards to the impact of cyberattacks throughout the world. According to the FBI's 2020 Internet Crime Report, there was a significant increase in complaints of suspected internet crimes in comparison to the previous year and losses that amount to billions of dollars. More so, deeper searches lead to ridiculous numbers supporting and justifying, the dread that many entities have towards the world of cybersecurity. As a matter of fact, this numbers might not even be close to the actual values by the simple fact that many companies and individuals tend to hide or wrongfully disclosure information regarding cyberattacks [6]. Notably, data breaches are often the cause for the concealment to the public, in order to mitigate any repercussions to an organization or individual.

Amidst the continuous approaches regarding cyberattacks, individuals are often classified based on their motivations [7]. On the other hand, and contrary to many, while they are divided by such designations, many share the same knowledge and set of tools.

This survey aims to deconstruct cyberattacks, by thoroughly covering hacking analysis, or attack analysis, and mitigation techniques. Moreover, the technical concepts will be followed with a practical application, that can be accompanied by anyone, independently of how knowledgeable they are on the matter.

2 Cybersecurity

A variety of concepts regarding the cybersecurity domain turn out to not only be hard to define but to explain due to their nature. As a concept that has changed through time, cyberspace is a perfect example [8]. In 2018 JP 3-12, DOD, the Pentagon released a term that would describe cyberspace as "the global

domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers" [9]. Such description was later accepted by some and refused by others, yet that isn't the point. The important part is to realize its correlation with cybersecurity, to further understand the consequent topics. In short, cyberspace is a critical infrastructure that holds information that is stored, shared, and communicated, a world of computer networks and its users [8]. When we engage with cyberspace, cybersecurity plays a huge role. The nature of the activities performed and involving cyberspace shape the necessity of cybersecurity, and whatever measures are applied when we engage with this world, they must support confidentiality, integrity, availability, and non-repudiation [10].
Nonetheless, securing something is about protecting it from the threats that could exploit its vulnerabilities [11]. Thus, the need to dispense any necessary resources to cybersecurity, and the required thought on how to steadily improve it. Striving for the utmost safety of our systems, organizations, and ourselves.

3 Hacking and Cybercrime

While cybersecurity has the constant need to keep up with the evolution of modern technology, attack analysis follows the trail of the increased complexity, severity, and events of cyberattacks [12].

First things first, taking each concept one by one, there is hacking. It's a scary term for many, yet an exhilarating sound for others. The word hacking, or hacker, didn't mean any harm a long time ago [13]. It was a way for individuals to either test their skills, or enjoy learning about the latest technology, but it doesn't represent that group of people anymore [13], not to the media at least. Hackers are now divided and described in various terms, all of them representing individuals in their differences, be it motivation, experience, or other [7]. The following denominations and respective descriptions, elaborate more about some of the existing types of hackers [14] [15].

- Black Hat: Contrary to White Hackers, this set of individuals are cybercriminals that intend to harm a computer system or network. They do so by stealing data, shutting down services, and more. Criminal communities where these cybercriminals interact and trade can be seen in the clear and dark web.
- Grey Hackers: Grey Hackers can be seen as both a Black Hat and a White Hack. They tend to decide on which hat will they wear for a certain job, depending on the best offer. This behavior is a major reason why many consider them one of the most dangerous types of hackers.
- White Hat: White hackers are also known as Ethical Hackers. They are security experts and a major strength to an organization's security team.

Shifting the focus to cyberattacks, these are the type of attacks carried out by cybercriminals. The European Union Agency for Cybersecurity, ENISA, released their Threat Landscape 2021 not too long ago [16]. Its documentation provides a well around update on many aspects surrounding this year's cyberthreats and cyberattacks. A resume of some of the content detailed in the Threat Landscape 2021 document is presented below [16]:

- Cyberattacks with nature in malware are still one of the major threats to today's entities.
- Hacktivism remains low yet impactful. It is mainly targeting specific organizations while maintaining their signature means of performing cyberattacks, like DDoS attacks and the release of sensitive data. A famous example of a hacktivist group is Anonymous.
- Conti was the ransomware with the highest monetary gain in 2021, going over 12 million dollars.

It also mentions the changes in cybercrime caused by COVID-19. Amidst the pandemic, many studies, and reports [17] have shown an increase in cybercrime since its early stages. Interpol COVID-19 Cybercrime Analysis Report [17], 2020, showcased data that would resonate in an alarming increase in cybercrime, involving phishing, ransomware on critical infrastructures, and overall, a group of cybercriminals exploiting people's weakness at unfortunate times. Even so, cybercrime events have been around for a long time and can carry out cyberstalking and cyberterrorism activities [18].

Nonetheless, there are still worldwide occurrences that showcase the positive side of hacking. Capture the Flag (CTF), in the scope of cybersecurity, are one of the many types of competitions that involve hackers. It is a great way to be part of the community while testing your skills and having a good time. Computer scientists, for example, have a lot to gain by being part of hacking conferences. Even more, many companies have been joining the world of bug bounties, congratulating hackers through monetary gains, most of the time, while improving the overall security of the business.

4 Hacking or Attack Analysis

Given the nature of cyberattacks, we can describe their analysis based on two points of view. We can view and approach a cyberattack in an offensive or defensive manner, each having its unique yet related set of methods. Although they can be divided by such terms, their motives shouldn't be assumed. An offensive approach can be taken to perform a security evaluation of a system, leading to an outcome that won't be considered a cybercrime. On the other hand, offensive methods can be used to deliberately make a cyberattack harder to fight against.

Depending on the perspective, we can think of attack analysis as the artistry that deconstructs a cyberattack, being that the overall goal is not only to identify it but to understand it [19]. Furthermore, it is crucial to mitigate its damage, if complete elimination of the problem isn't possible.

The methods of how attack analyses are carried out can vary depending on multiple factors, such as the nature of the cyberattack or the operating system of the targeted machine. [19] In the eventuality that an attack has occurred and we are aware of such, forensic analysis can help us better understand what happened by searching for possible actions made by the hacker, while also deducing the damage caused. If legal actions were to be taken, it is also possible to gather evidence for such, although a countermeasure could be used by the cybercriminal to prevent any traceable information, and make our work of analysis harder.

To achieve a certain level of complexity, we will focus on a specific type of cyberattack and base our hacking analysis and attack analysis on the respective. Being malware a great enemy to cybersecurity in today's century, it will become the focus of the next topics.

A dynamic or static approach are both ways to conduct malware analysis, where the difference lays down on whether we run the malware while we examine it or not [20]. Furthermore, we can describe them as basic or advanced.

Table 1. Approaches to Malware Attack Analysis

Basic Static Analysis	A basic and quick way to gather information. Not that effective towards advanced malware.
Basic Dynamic Analysis	Analyse based on monitoring the malware in action. It's recommended to proceed with the necessary tasks in a safe environmnent.
Advanced Static Analysis	A more in-depth analyse, usually involving dissembling tools.
Advanced Dynamic Analysis	May provide information that might have escaped previous techniques

Both basic type analyses could be done by everyone, even the newcomers to the field. It can be an effective way to identify and apply measures to eliminate malware lacking in complexity. It is recommended that when running the dynamic analysis, the process should be executed in a safe environment, often called sandbox, to prevent damage to the main network and system. The advanced static analysis provides a clear understanding of what we are dealing with [20]. A great and helpful tool for this task, that involves assembly language is IDA Pro. If none of the techniques above seem to be giving the desired, or necessary information, then advanced dynamic analysis might be the answer. Usually, they are done through debugging to better deconstruct the running executable.

Below are introduced ways to gather information from executables, which are usually what we will be facing when analyzing malware [19]:

- Antivirus tools.
- Hashes for malware identification.
- File strings analyze

Out there, most antivirus software adopts one of these two methods: Signatures, Heuristic Analysis [21]. Those who follow the signature route, work by comparing the piece of viruses with a signature database,

to see if it finds a match [21]. A big problem with the described method is that there is always a possibility of no match being found, even though it is analyzing a virus. However, the heuristic method doesn't stop at the code and tries to go further. It looks to predict and learn its behavior, often utilizing machine learning techniques [22].

To those who are unfamiliar with hashing, it is a great way to identify malware. One could describe hashing as an algorithm applied to data, such as a file, that later produces a unique hash [23]. You could think of this unique hash as a fingerprint that identifies the malware. This hash code can then be helpful to carry out further investigation. Below are listed two popular cryptographic hash methods [24]:

- MD5
- SHA

Although SHA is considered more secure, MD5 has the upper hand when it comes to speed [25]. Some similarities can be seen in regards to padding and resource utilization [25].

A string is a term that is very common in programming. It can be described as a sequence of characters, and while they reside inside files, extracting them can give crucial information about the binary in question [26]. It has proven to be a very efficient method for static analysis [27].

Regarding the offensive approach, although hackers vary concerning the reasons for their actions, they tend to share the way, and means of how they plan, and conduct their activities.

Table 2. Types of Hacking and respective tools

Port Scanners	Nmap
	Auto scan
Packet Sniffers	Wireshark
	TCPdump
Vulnerability Exploitation	Metasploit
	Social Engeneering ToolKit
Intrusion Detection Systems	Snort
	Netcap

As a matter of fact, Table 2 shows several techniques that are used for both offensive and defensive tasks, leaning more towards an ethical hacker approach [28].

5 Mitigation Techniques

New signatures, patches, and many more variables maintain as an imminent threat towards mitigation techniques effectiveness [29]. These techniques address multiple mechanisms to elevate its efficiency, such as [29]:

- Detection;
- Response;
- Tolerance.

Although there is a vast number of mitigation techniques out there, many studies, and reports from various entities have addressed crucial, and popular mechanisms that are approached independently of the threat that is being considered. Abstracting from the topic of the survey, we can describe mitigation as they diminish in harm or loss caused by some sort of unwanted event. On the other hand, prevention leans more towards guaranteeing that the unwanted event never happens, although some may further describe the term prevention and acknowledge that in some cases, it does look to reduce the negative impact of such situations.

Therefore, it is safe to view mitigation techniques in correlation to cybersecurity as any means or methods that lead to reducing the damage caused by a cyberattack. Such techniques will overview prevention, detection, remediation, and response mechanisms, to better mitigate any harmful tragedies.

The FBI Ransomware Prevention and Response for CISOs [30] is one of the many artifacts that will, in a way or another, end up touching on the following subjects when it comes to prevention:

- Training with a focus on threats and attacks awareness;
- Patching operating system and software;
- Advanced configuration of firewalls related to IP addresses;
- Managing access controls;
- Implementation of Security Policies.

Following the same structure as Hacking Analysis, mitigation techniques will be further analyzed with the usage of a cyberattack.

In the middle of 2014, a banking Trojan made its appearance. The so called Emotet is a malware that upon gaining access to the victims machine, it would gather information and communicate the same to a command and control infrastructure (C2 or C&C) [31]. Known to be a major threat to the financial sector in 2019 [32], the infection process would start by users opening a Microsoft Word document, earlier received through email, and upon clicking on the agreement displayed to them, the macros would activate the Emotet malware, using HTTP POST to send data from the victim's computer [31]. Regarding the financial sector, it was a major threat to the respective in 2019 [32]. Below there are listed a few mitigation measures that can be applied to protect against a malware with similar behavior:

- Blocking email attachments that can't be scanned by an antivirus software.
- Disabling file sharing services.
- Scanning suspicious email attachments.
- Implementing the suitable Access-control lists

6 Case Study

For study purposes, we will not formulate a plan to lure the victim into being attacked, but rather use a malware sample and let ourselves get attacked. This study will focus on attack analysis, from a defensive approach, covering both static and dynamic malware analysis that can be performed by everyone, independently of their knowledge on the matter.

For starters, an adequate way to boost the safety of our machine when analyzing malicious software is the use of a virtual machine. Virtualization has been steadily increasing in popularity, and it can both be used by the hacker and the defender, or victim. A virtual machine can be seen as a computer inside another computer, and it's a great way to minimize the potential damage to our main system. Furthermore, another key factor to be aware about is the network. As a defender and future malware analyst, we do not want to compromise our network. Since a malware can easily spread through a network, and proceed to infect other connected devices, this is of utmost concern. Nonetheless, we don't want to completely isolate the malware from the internet but is a key thought to keep in mind.

Following the construction of the lab, our safe environment to run the malware, we initially created a virtual machine, using the VMware software. Then, on that machine, it was installed the Windows 10 Operating System. After the installation process, it's time to download the necessary tools to do malware analysis. It's after this step that we can proceed with the configuration of the lab in ways that it won't affect the network, as previously intended.

The default network configuration has (NAT) as the Network Adapter. This was important to allow the download of the necessary tools to perform malware analysis. Now, we will change it and go a step further. One way of thinking about how one can protect a network when performing malware analysis, is to simply cut any connection to the internet. While this idea isn't necessarily the worst, a variety of malware require internet connection to act has they were designed to. If we want to understand and properly analyze the malware, we still have to allow some connection, yet find a way to control the malicious software. That's the usefulness of host-only networking. Host-only networking creates a connection between the guest and the host, containing the malware in the virtual machine while allowing some access to the internet. This way, we can better analyze it and understand what it does, like downloading other malware from the internet. Another step further would be the usage of multi virtual machines over the same concept, but it wasn't the method applied in this study.

The necessary precautions were made, and its now time to start shifting our focus to the malware. As a note, those were two main configurations that were needed in order to significantly boost our chances of guaranteeing security to our system and network, yet there are others who were taken in consideration. Version and updates of the used softwares, shared folder configurations, and USB connected devices are some of those.

Due to the nature of the chosen operating system, the antivirus that is currently working on the virtual machine is the Windows Defender. For study purposes, we want the malware to enter our system so we will be disabling Windows Defender.

The chosen samples required a password between the process of downloading them, and installing them. This is a helpful method to mitigate human error incidents when it comes to mistakes in this process.

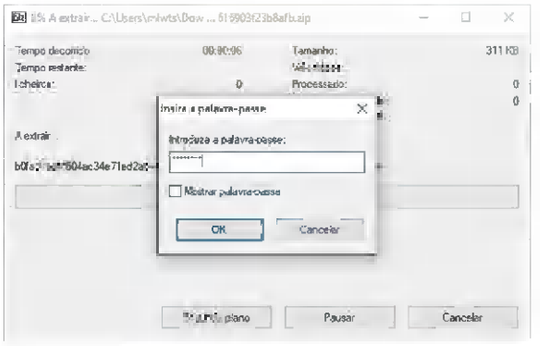

Fig. 1. Malware Sample

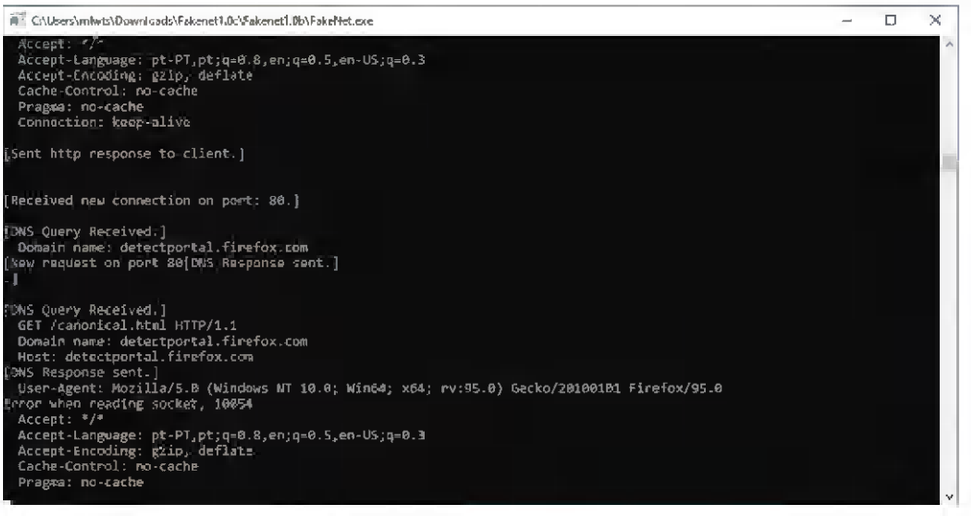

Fig. 2. Running fakenet

Furthermore, we use fakenet to trick the malware into thinking that the machine isn't isolated from the main network. It rises our chances of bypassing whatever methods the malware might have to detect if we are in environment systems or not.

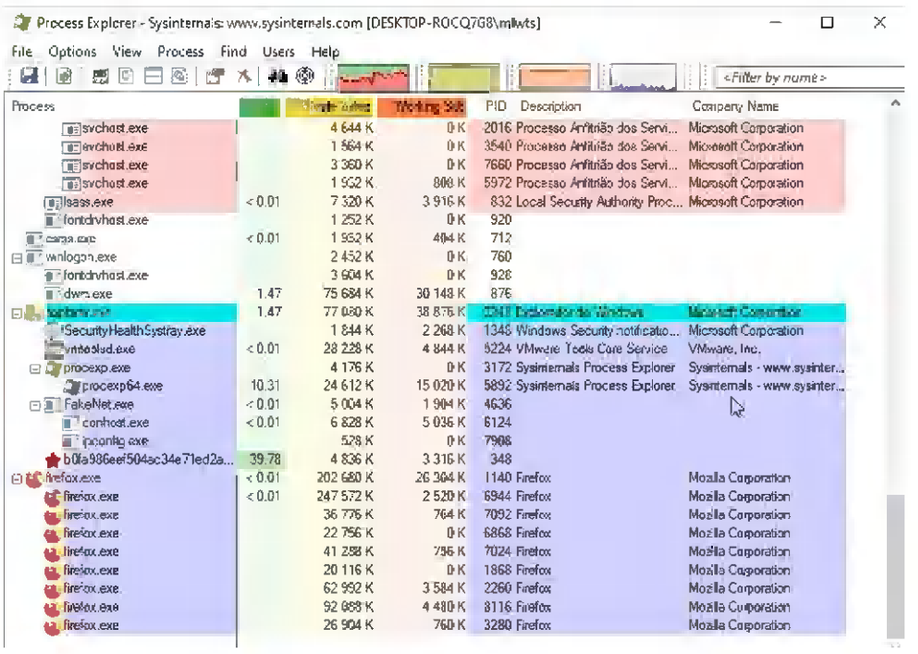

Fig. 3. Process Explorer after executing the malware

The Process Explorer is a notable tool for us to understand in real time what is happening in our system. Just from this view we can check a Process name, his description, if has any, company name, and more. If we look further into a Process, we are faced with a GUI about the respective that provides us with even more detail, such as strings and signatures.

Fig. 4. Malware Process

Regshot allows us to create two shots that will monitor every change in the system between their activation. It is an amazing way to spot what changed after we run the malware. A report at the end can be made with the changes by the Comparing setting.

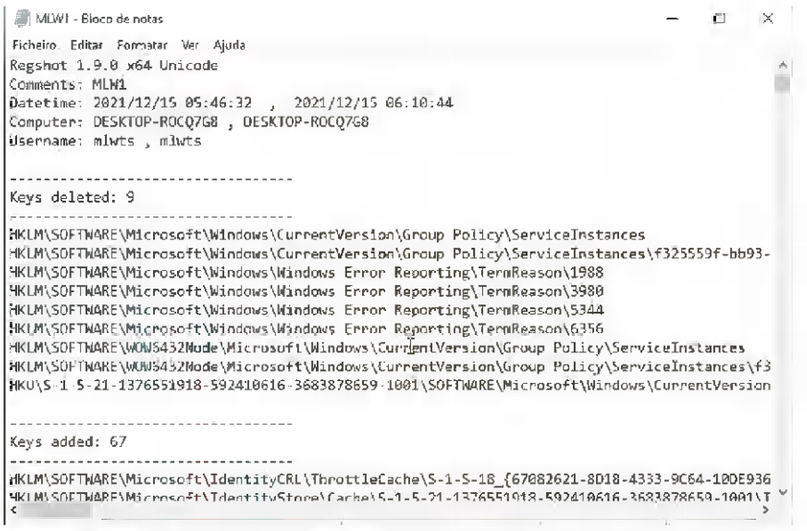

Fig. 5. Regshot Report

The information in the note is the result of the "Compare" feature in Regshot. There were a total of 309 changeswith values being changed, keys deleted and more.

Shifting back to static analysis, the MD5 hash code is the following.

Fig. 6. MD5 command and Hash

We do so in cmd, by first changing directories to the tool repository. Afterwards, we insert the following command with first, the hashing tool md5deep, and then the malware. The MD5 code was the following: 34568261ff17bda650f7c50d607fad4e.

To analyze the strings we can use the strings tool.

Fig. 7. String command

We will need to changed directories to the repository of the strings tool. We then want to run the command with the word strings, followed by the path to the malware.exe file. The following images represent portions of what was shown in the command line.

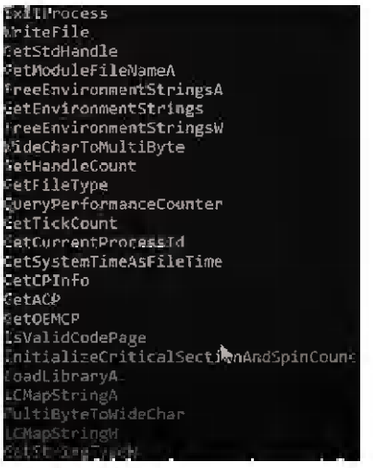

Fig. 8. Strings command outcome

The information gathered to this point was enough to have a slight understanding of this malware. It was a culmination of both static and dynamic analysis, although further investigation could be done to understand it to its fullest, while obviously requiring a deeper understanding of concepts such as dissembling. Nonetheless, we can still gather even more information by doing a search on google with the gathered data.

We can either use MD5 or SHA-1 that we retrieved from malware and check if other entities have performed analysis on this sample. As of today, this malware has been classified as suspicious by many individuals according to the website Virustotal.

7 Conclusion

Amidst the on growing surge of cyberattacks, attack analysis and mitigation techniques have shown to significantly affect the outcome of today's systems and networks security issues. Although they are generally seen as fields where only high knowledgeable individuals on the matters would succeed, there are many ways one without notable fundamentals on the subject could improve their security in regard to the mentioned network and system. The agglomerate of tools and means may be equally present in the process of a cyberattack, incident response and vulnerability check, be it to scan ports on a company's network or ARP spoofing to intercept communications.

Intending to properly understand the concepts involved in the practical demonstration, there was a first introduction to cybersecurity followed by a more focused view on attack analysis and mitigation techniques, acquiring knowledge on static and dynamic analysis for a more defensive approach. Moreover, it was introduced some tools which uses can be both for a defensive and offensive procedure.

Noteworthy, all entities that are in the slightest affected by the phenomenon's involving cybersecurity should look to continuously adapt their systems, networks, and knowledge as a means to fight back the never-ending changes and evolution of cyberattacks.

As for a future paper, going over a practical application of an offensive approach to a system or network would result in a more solid cybersecurity work. Further describing and analyzing cyberattacks would also significantly raise awareness for the possible damage derived by all the types of cyberattacks.

References

1. Sutherland, Ewan, Cybersecurity: Governance of a New Technology (March 26, 2018). Proceedings of the PSA18 Political Studies Association International Conference. Cardiff, 26-28 March 2018, Available at SSRN: https://ssrn.com/abstract=3148970 or http://dx.doi.org/10.2139/ssrn.3148970
2. SPIDALIERI, Francesca. State of the States on Cybersecurity. Pell Center for International Relations, 2015.
3. Capelão, F.; Barbosa, H.: "Cybersecurity in Healthcare: Risk Analysis in Health Institution in Portugal", International Journal for Research & Development in Technology (IJRDT), vol. 9:3, pp. 25 -31, (2018)
4. Clarke R, Youngstein T. Cyberattack on Britain's National Health Service - A Wake-up Call for Modern
5. CASHELL, Brian, et al. The economic impact of cyber-attacks. Congressional research service documents, CRS RL32331 (Washington DC), 2004, 2.
6. KIM, Bokyung; JOHNSON, Kristine; PARK, Sun-Young. Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. Cogent Business & Management, 2017, 4.1: 1354525.
7. YAACOUB, Jean-Paul A., et al. A Survey on Ethical Hacking: Issues and Challenges. arXiv preprint arXiv:2103.15072, 2021.
8. SINGER, Peter W.; FRIEDMAN, Allan. Cybersecurity: What everyone needs to know. oup usa, 2014.
9. Department Of Defense (2018), JP 3-12, Cyberspace Operation, Washington, DoD.
10. KOSTOPOULOS, George. Cyberspace and cybersecurity. CRC Press, 2017.
11. VON SOLMS, Rossouw; VAN NIEKERK, Johan. From information security to cyber security. computers & security, 2013, 38: 97-102.
12. UMA, M.; PADMAVATHI, Ganapathi. A Survey on Various Cyber Attacks and their Classification. Int. J. Netw. Secur., 2013, 15.5: 390-396.
13. PALMER, Charles C.. . Ethical hacking. IBM Systems Journal, 2001, 40.3: 769-780.
14. Richet, J. L. (2012). How to Become a Black Hat Hacker? An Exploratory Study of Barriers to Entry into Cybercrime (No.hal-02187741)
15. SAHARE, Bhawana; NAIK, Ankit; KHANDEY, Shashikala. Study of ethical hacking. Int. J. Comput. Sci. Trends Technol, 2014, 2.4: 6-10.
16. ISBN: 978-92-9204-536-4 – DOI: 10.2824/324797 – ISSN: 2363-3050
17. Interpol,https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

18. GORDON, Sarah; FORD, Richard. On the definition and classification of cybercrime. Journal in Computer Virology, 2006, 2.1: 13-20.
19. SIKORSKI, Michael; HONIG, Andrew. Practical malware analysis: the hands-on guide to dissecting malicious software. no starch press, 2012.
20. PRAYUDI, Yudi, et al. Implementation of malware analysis using static and dynamic analysis method. International Journal of Computer Applications, 2015, 117.6.
21. Shevchenko, Svitlana & Skladannyi, Pavlo & Martseniuk, Maksym. (2019). ANALYSIS AND RESEARCH OF THE CHARACTERISTICS OF STANDARDIZED IN UKRAINE ANTIVIRUS SOFTWARE. Cybersecurity: Education Science Technique. 62-71. 10.28925/2663-4023.2019.4.6271.
22. BAZRAFSHAN, Zahra, et al. A survey on heuristic malware detection techniques. In: The 5th Conference on Information and Knowledge Technology. IEEE, 2013. p. 113-120.
23. SIHWAIL, Rami; OMAR, Khairuddin; ARIFFIN, Khairul Akram Zainol. A survey on malware analysis techniques: Static, dynamic, hybrid and memory analysis. International Journal on Advanced Science, Engineering and Information Technology, 2018, 8.4-2: 1662.
24. CHI, Lianhua; ZHU, Xingquan. Hashing techniques: A survey and taxonomy. ACM Computing Surveys (CSUR), 2017, 50.1: 1-36.
25. Kumar, Sandeep & Gupta, Er Piyush. (2014). A Comparative Analysis of SHA and MD5 Algorithm. International Journal of Computer Science and Information Technologies. 5. 4492 - 4495.
26. Mohamed, G. A. N. & Ithnin, N. B. (2017). Survey on Representation Techniques for Malware Detection System. American Journal of Applied Sciences, 14(11), 1049-1069.
27. Lee, Jinkyung & Im, Chaetae & Jeong, Hyuncheol. (2011). A study of malware detection and classification by comparing extracted strings. 75. 10.1145/1968613.1968704.
28. KUMAR, K. Pavan; PRANATHI, K. A Survey on Ethical Hacking, Approaches, Attacks, Procedure & Reliability in case of Cyber Crime.
29. MAHJABIN, Tasnuva, et al. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks, 2017, 13.12: 1550147717741463.
30. FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view
31. KURAKU, Sivaraju; KALLA, Dinesh. Emotet Malware—A Banking Credentials Stealer. Iosr J. Comput. Eng, 2020, 22: 31-41.
32. KELLERMANN, Tom; YOUNG, B. Modern Bank Heists: The Bank Robbery Shifts to Cyberspace. Technical report, Carbon Black, OPTIV, 2019.
33. TUFAIL, Shahid, et al. A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. Energies, 2021, 14.18: 5894.
34. HAWAMLEH, A. M. A., et al. Cyber Security and Ethical Hacking: The Importance of Protecting User Data. Solid State Technology, 2020, 63.5: 7894-7899.
35. SHABUT, Antesar M.; LWIN, Khin T.; HOSSAIN, M. Alamgir. Cyber attacks, countermeasures, and protection schemes—A state of the art survey. In: 2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA). IEEE, 2016. p. 37-44.
36. HOQUE, Nazrul; BHATTACHARYYA, Dhruba K.; KALITA, Jugal K. Botnet in DDoS attacks: trends and challenges. IEEE Communications Surveys & Tutorials, 2015, 17.4: 2242-2270.
37. FEILY, Maryam; SHAHRESTANI, Alireza; RAMADASS, Sureswaran. A survey of botnet and botnet detection. In: 2009 Third International Conference on Emerging Security Information, Systems and Technologies. IEEE, 2009. p. 268-273.
38. PRAYUDI, Yudi. THE RECOGNIZE OF MALWARE CHARACTERISTICS THROUGH STATIC AND DYNAMIC ANALYSIS APPROACH AS AN EFFORT TO PREVENT CY.. Journal of Theoretical and Applied Information Technology, 2015, 77.3.
39. PATTEN, David. The evolution to fileless malware. Retrieved from, 2017.
40. HAMED, Zakaria A.; AHMED, Ibraim M.; AMEEN, Siddeeq Y. Protecting windows OS against local threats without using antivirus. relation, 2020, 29.12s: 64-70.
41. Alenezi, Mohammed & Alabdulrazzaq, Haneen & Alshaher, Abdullah & Alkharang, Mubarak. (2020). Evolution of Malware Threats and Techniques: A Review. International Journal of Communication Networks and Information Security. 12. 326.
42. BARIK, Mridul Sankar; SENGUPTA, Anirban; MAZUMDAR, Chandan. Attack Graph Generation and Analysis Techniques. Defence Science Journal, 2016, 66.6.
43. TEOH, Chooi Shi; MAHMOOD, Ahmad Kamil; DZAZALI, Suhazimah. Cyber Security Challenges in Organisations: A Case Study in Malaysia. In: 2018 4th International Conference on Computer and Information Sciences (ICCOINS). IEEE, 2018. p. 1-6.
44. AURANGZEB, Sana, et al. Ransomware: a survey and trends. Journal of Information Assurance & Security, 2017, 6.2: 48-58
45. N. Kshetri and J. Voas, "Hacking Power Grids: A Current Problem," in Computer, vol.50, no. 12, pp. 91-95, December 2017, doi: 10.1109/MC.2017.4451203.
46. AURANGZEB, Sana, et al. Ransomware: a survey and trends. Journal of Information Assurance & Security, 2017, 6.2: 48-58

47. Kruse CS, Frederick B, Jacobson T, et al. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technol Heal Care 2017;25:1–10. doi:10.3233/THC-161263
48. Sutherland, Ewan, Cybersecurity: Governance of a New Technology (March 26, 2018). Proceedings of the PSA18 Political Studies Association International Conference, Cardiff, 26-28 March 2018
49. D. K. Alferidah and N. Jhanjhi, "Cybersecurity Impact over Bigdata and IoT Growth," 2020 International Conference on Computational Intelligence (ICCI), 2020, pp. 103-108, doi: 10.1109/ICCI51257.2020.9247722.
50. SPIDALIERI, Francesca. State of the States on Cybersecurity. Pell Center for International Relations, 2015.
51. Kuraku, Sivaraju & Kalla, Dinesh. (2020). Emotet Malware -A Banking Credentials Stealer. 10.9790/0661-2204023140.