COMMON TYPES OF CYBER-ATTACK AND METHODS OF DEFENCE

CENG 3544, COMPUTER AND NETWORK SECURITY

Oğulcan Bulut
ogulcanbulut3@posta.mu.edu.tr
Muhammad Rafi Khudayar
rafi.khudayar@gmail.com

Sunday 5th June, 2022

Abstract

With everyday passing by we bond with the technology more and more, even now we are in a point that most of us are inseparable with technology. Most people can't imagine living without it. It is all because of the non-physical world created by the Internet. As this non-physical or cyber world grows so does the rate of cybercrimes and cyber criminals. And every day new types, techniques, and tools of cyber-attacks come along. There are many types of cybercrime such as child pornography, drug dealing, types of cyber-attacks and many more. The intention of this project is to cover some common types of cyber-attacks and ways to defend against them.

1 Introduction

First of all, let's have a definition of what a cyber attack is. As the name suggests a cyber-attack is an attack or "an assault launched by criminals using one or more computers against a single or multiple computers or networks. A cyber-attack can maliciously disable computers, steal date, or use a breached computer as a launch point for other attacks." In other words, a cyber-attack is a way of gaining unauthorised access to a network, or bunch of data with the intentions of compromising the confidentiality, integrity, availability, and authenticity of information. "Cyber-attacks can be associated with cyber warfare or cyber-terrorism". The motivation behind these attacks are mainly divide in three categories:

- Criminal: In case of criminally motivation, attackers are after data theft such as bank account information, and personal data. Financial gains such as stealing money or transferring money to other accounts without the knowledge of the account owner. And business or government systems disruption in which the attacker aim for the systems.
- Personal: For the personal motivation part, attacker try to take revenge for their personal beliefs or a grudge they have against a company or a specific person.
- Political: Lastly, the motivation behind the political scenario is to prove a point or seek attention for a cause. That's why they make their attacks known to the public, this action is considered as hacktivism as well.

Cybercriminals take advantage of methods such as malware, phishing, ransomware, denial of service and other methods to launch a cyber-attack. Indeed, there are ways to defend against these attacks and have more secure systems, yet this remains a fact that there is no 100% security in a cyber-space. In addition, the securer a system gets the slower it will be because of all the security protocols.

2 Most common types of cyber-attack

2.1 Malware

A malware is the shortened form of "Malicious Software" which refers to any intrusive software developed by criminals or hackers. The motivation behind developing such software is to steal data damage computers and systems. Malwares affects a system or a computer through the vulnerabilities where a user opens a dangerous or a third-party link received through social media, e-mail, or a USB device which in result the malware gets access to the system. There are many types of Malwares with different characteristics as explained in the following part:

2.1.1 Virus

Almost everyone who uses or have used a computer has come across computer viruses and had fist hand experience. "Viruses are a subgroup of malware." It is a malicious software that is attached to a file or a document that is executable and runs. In other words, a virus is a malicious code that runs on system after being executed by a user. It runs without the permission of the owner right after getting access to it and it spreads from system to system. "Viruses can disrupt system's ability to operate. As a result, they cause significant operational issues and data loss." Some dangerous viruses in the history have been listed below:

- Mydoom
- Sobi
- Klez
- ILOVEYOU
- WannaCry
- Zeus

2.1.2 Worms

Another type of malware is worms "that rapidly replicates and spreads to any device within a network. Unlike viruses, worms do not need host programs to disseminate. A worm infects a device via a downloaded file or a network connection before it multiplies and disperses at an exponential rate." The same as viruses, worms too disrupt devices and cause data loss.

2.1.3 Trojan virus

"Trojan viruses are disguised as helpful software programs." However, once they are inside a system, they can gain access to sensitive data and can modify, block, or delete the data. This causes harm to the infected system and decrease the performance of the system significantly. In addition, they do not self-replicate.

2.1.4 Ransomware

"Ransomware is sophisticated malware that takes advantage of system weaknesses, using strong encryption to hold data or system functionality hostage." And the user cannot access the information. Cybercriminals use ransomwares to demand financial pay-outs for releasing the data.

2.1.5 Fileless malware

"Fileless malware if a type of memory-resident malware." This type of malware resides in the computer's memory not in the hard drive and operates from there. Since there are no files to scan, it is way difficult to detect a fileless malware. In addition, when the infected computer reboots the malware disappears, which makes it more difficult for the forensics as well. A recent example of fileless malware is the FritzFrog. FritzFrog is a fileless peer-to-peer botnet malware that is designed to infect systems with the intention of mining cryptocurrency. FritzFrog was detected in August 2020.

2.2 Phishing

Phishing is the practice of sending fraudulent communications from a trustworthy source usually through emails. The goal of this method of attack is to breach a system and gain access to your online accounts and personal data, obtain permissions to modify and compromise connected systems. In addition, cybercriminals aim to install malwares on a system, steal sensitive data, do financial fraud. Phishing is one of the most common ways of cyberattacking proven in the history of digital world. The simplicity and ease of tricking users into phishing makes it very successful way of cyber-attack. Emails that affect emotions such as fear, curiosity, and urgency are sent to victims and expected to fool them by clicking the links or providing confidential.

- A study has suggested that in 2020, phishing attacks increased during the COVID-19 pandemic, because of Black Friday, Cyber Monday, and online shopping.
- According to the CSIS:" In May 2022, A phishing campaign targeted the Jordan Ministry of Foreign Affairs. Researchers attributed the attack to an Iranian cyber espionage actor."

2.3 Man-in-the-middle

Man-in-the-middle (MitM) attack is a type of attack that the attacker gains access to the communication of the client and the server and learns all the data about that communication. This attack is called as eavesdropping attack as well. This kind of attack makes a threat actor to seize, sent and receive the data which intended for someone else others. The integrity, confidentiality, and authenticity of data is aimed in this attack.

The stage that a encourages a Man-in-the-middle attack are such as: unsecure public WI-FI, where it is very easy for attackers to get access to, and an infected system especially with a malware. Either the malware itself acts as an agent for the MitM attacker or it install another software that does the job.

2.4 Denial-of-service (DoS) and Distributed-denial-of-service (DDoS)

A Denial-of-service (DoS) attack floods a system, server, or a network with traffic with the intention of exhausting resources and services which, results in significant drop in the performance. Distributed-denial-of-service (DDoS) is similar to DoS attack with the only difference that in DDoS the attackers use many compromised devices to attack the target instead of one. DoS and DDoS attacks are among the most dangerous and most difficult types of attack to prevent. In addition, differentiating is from the normal traffic request is very challenging as well.

2.5 SQL Injection

Structured Query Language (SQL) injection is an attack that the attacker uses a malicious SQL code to a server through vulnerable applications. The target of this attack is data servers which they reveal information if the attack is successful. HTML forms and search boxes are more vulnerable against this attack.

2.6 Zero-day exploit

Zero-day exploit hits after a network vulnerability is announced, yet, before a patch or a solution is found. The attackers take advantage of the time that the attack is announced, and it is patched to get to a system. This type of attack take time to get discovered and patched. Sometimes it gets up to a year before developers find out about a zero-day exploit.

3 Ways to defend against cyber-attacks

3.1 Malware

3.1.1 Virus

In order to protect against computer viruses, antivirus software is often used. Antivirus software can be separated into two categories, which are network antivirus software and standalone antivirus software. The former detects when a virus invades a network and deletes it, while the latter is often installed on personal computers.

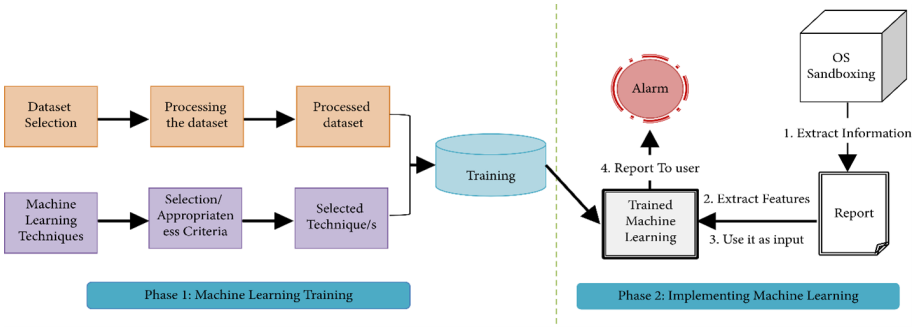
3.1.2 Worms

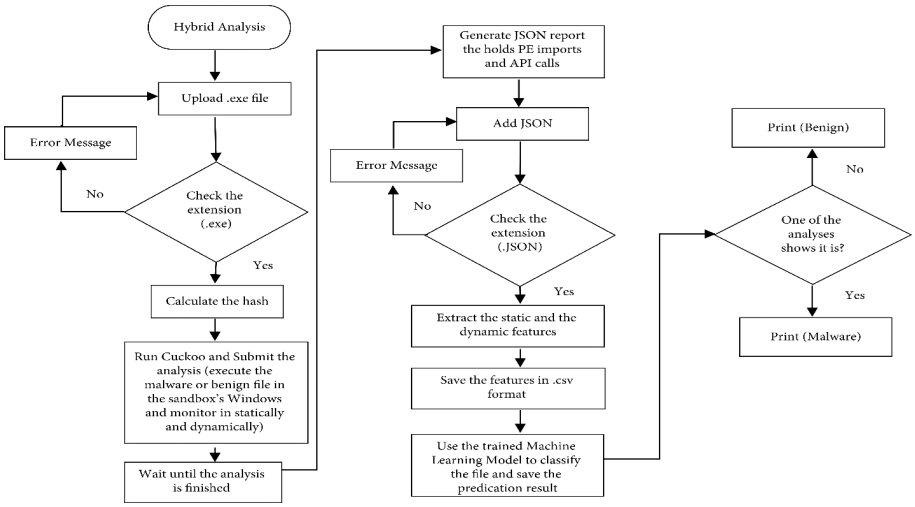
There are many different techniques to defend against worms, one of which is by using traffic dispersion graphs in order to model the traffic of a network and train the detection systems. Another technique is the use of casual-tree worm propagation, which factors in graph metrics such as branching factor and depth, behaviour so that the system can detect worm attacks. Then there are also techniques like internet control message protocol (ICMP), distributed anti-worm (DAW) architecture. These techniques can be considered limited by the fact that they can only detect certain types of worms and only after a certain amount of infection has already taken place, and they also require a large amount of resources to work properly.

3.1.3 Trojan virus

One method used in detecting Trojan viruses combines both dynamic analysis, which analyse the behaviour of the malicious code once it is inside the system and makes a call when a specific event is triggered, and static analysis, which puts signature detection technology to

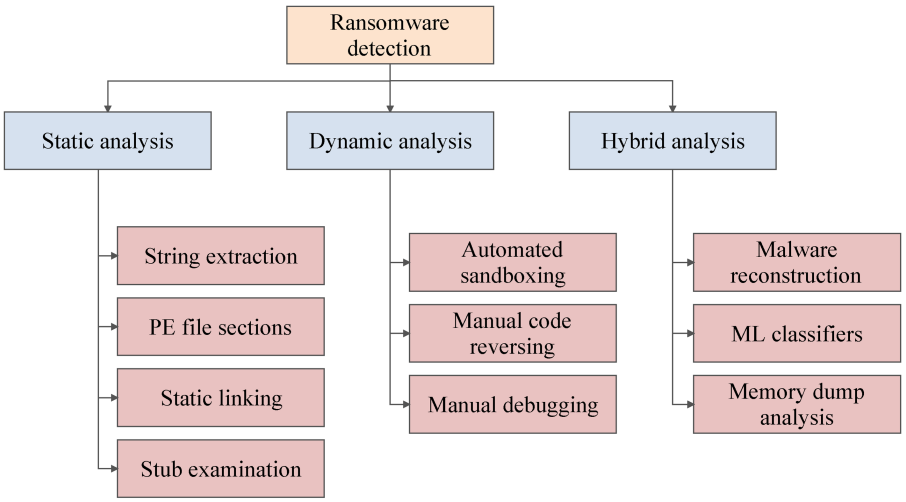
use to compare and analyse the characteristics to the ones that are already collected. Another method used to defend against Trojan viruses is called ZeVigilante. This particular model takes advantage of machine learning from various datasets and after implementation it starts testing.





3.1.4 Ransomware

DAM Framework is one of the proposed methods of defence against the notorious ransomware software in the past few years. Same as many other defence methods out there DAM Framework also utilizes static, dynamic and hybrid analysis, all of which then branches off into different techniques. The detection system used in the proposed technique can be observed in more detail in the following figure.



One of the future directions that DAM Framework intends to take is making browsers a first line of defence against ransomware software as users download files via browsers as there hasn't been any steps taken yet to make browsers able to detect a ransomware inside themselves or just make them adequate to give the user a simple warning.

3.1.5 Fileless malware

Software such as Comodo Advanced Endpoint Protection, Cytomic and BlackBerry Cylance are often used in defending against fileless malware. Comodo also offers Host Intrusion Prevention System (HIPS) while Cytomic, with the help of Endpoint Prevention Detection and Response (EPDR) can help detect and react to any sort of malware.

3.2 Phishing

There are three main techniques to defend against a phishing attack, first of which is Rule-Based Phishing Detection. In Rule-Based Phishing Detection the whole system revolves around the ruleset, it can be limited in performance. Second technique is Machine-Learning Based Phishing Detection, in which the machine learning models take certain parts of a website (URL or HTML content) and then shape itself accordingly. The third of the main phishing techniques is Google Safe Browsing. Google Safe Browsing is basically a deny list that exists in popular browsers.

3.3 Man-in-the-middle

One of the proposed defending methods against man in the middle attacks is, by using already existing Bluetooth Low Energy (BLE) knowledge, to distinguish differences and inconsistencies between features and behaviours of devices.

The stage that a encourages a Man-in-the-middle attack are such as: unsecure public WI-FI, where it is very easy for attackers to get access to, and an infected system especially with a malware. Either the malware itself acts as an agent for the MitM attacker or it install another software that does the job.

3.4 Denial-of-service (DoS) and Distributed-denial-of-service (DDoS)

To defend against Dos/DDoS attack there are many ways, for example increasing the bandwidth, so that handling any kind of traffic spike created by attackers is possible. Also, using cloud-based solutions are a good way to decrease the risk of being attacked. In addition, installing intrusion-detection and prevention system (IDPS) is another way to avoid DoS and DDoS attacks, because IDPS detects the abnormality in the traffic and blocks it

3.5 SQL Injection

For SQL Injection there are many ways to defend as well. To start with, parametrising statements are a good practice, this method ensures that all the inputs passed in a SQL statement is safe and well treated. The next thing to do is, continuously updating all the infrastructure of a system. In addition, every system should have their own individual database, this decreases the risk of SQL Injection attack as well. A system should also have input checking and should only take characters as input that are required no extra or especial characters. This limits the user in inputting any kind of SQL query.

3.6 Zero-day exploit

Updating your system and regularly installing necessary patches ensures the security of the system against Zero-day exploit attack, however, it would not be enough, adding firewall, IDPS, and Antivirus is a good practice for keeping the system safe. Furthermore, preventing the spread of this attack is very important. To prevent the spread of Zero-day exploit limiting connections is required, this means that the connections with the top priority or that are necessary is allowed, all other connections are blocked.

4 Related Works

There are many research paper based on cyber-security, to be more specific on cyber-attacks and ways to defend against them. We will provide discuss some starting with the cyber-attacks and then ways to defend.

Attacking: With all the new technologies everyday emerges new ways of use misusing all these technologies. Cyber-criminals are always after vulnerabilities in these technologies. According to the Cisco Annual Cybersecurity Report the rate cyber attacks were four times grater during January 2016 and October 2017.

In addition, Centre of Strategic International Studies (CSIS) there have been thousands of cyber-attacks. This organisation has kept records of all the cyber-crime activities from 2006 to this date. They tend to keep their webpage regularly updated which a very important task.
In case of the questions, what a cyber-attack is? Or what types of cyber-attacks exist? These questions are answered very clearly, with details in the research paper done by Jibi Mariam Biju, Anju J Prakash, and Neethu Gopal under the name of “Cyber attacks and its different types”. We have addressed to the paper in the reference section.

Defending: Defending against a cyber-attack is a very important concept, that is why many researches are done regarding this subject. In a research conducted by Andreea Bendovschi emphasis on the importance of this topic and offers solutions for increased security.

5 Implementation

This report includes a small demonstration as well, they step by step demonstration will be explained here, however, the video that is prepared with this report will include the detailed demonstration. We intend to demonstrate a DoS attack. Not to mention, with DoS or DDoS attack, the attacker aims for the availability of a system or a network, and tries to bring the system done so that it is not available anymore.

The implementation has been done on a testing environment with only educational purposes.

To start with, we should have knowledge of the system we want to attack, and we use NMAP to gather information about the victim system.

- namp -A ip-address of the network we want to gather information about

After gathering information about a network, we should be able to see what ip address is up and has a running host. We should also check carefully the open ports and ip address of the host we want to attack.

At this stage we use hping3 which is a packet generator tool, and type:

- hping3 -S source-ip-address -a destination-ip-address -p port-address –type-of-attack.

At this stage the victim host is being flooded with the packets sent by our system, the victim system we start using more resources and significant drop of performance will be noticed.

6 Conclusion

To sum up, cyber-threats exist, and they are very dangerous, they can bring harm to the real world as well. A cyber-crime is done in a blink of an eye, or sometimes when no one knows about it until it is announced by the attacks. A cyber-attack can at any moment in our life since no one is away from technology, so we should be aware of all our online activities and try to use secure systems as much as possible. If we are responsible for the cyber-security of a company, we should always try to educate the personnel about the importance of cyber-security, and methods to minimize its risks.

References

[1] Andreea Bendovschi, Cyber-Attacks – Trends, Patterns and Security Countermeasures, 7th INTERNATIONAL CONFERENCE ON FINANCIAL CRIMINOLOGY 2015. 13-14 April 2015, Wadham College, Oxford, United Kingdom

[2] CYBER ATTACKS AND ITS DIFFERENT TYPES, Jibi Mariam Biju1, Neethu Gopal2, Anju J Prakash3 1,2Mtech, CSE Department, Sree Buddha College of Engineering, Kerala, India 3Assistant Professor, CSE Department, Sree Buddha College of Engineering, Kerala, India

[3] https://www.ibm.com/topics/cyber-attack

[4] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[5] https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/

[6] https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html# types-of-cyber-attacks

[7] https://www.hp.com/us-en/shop/tech-takes/top-ten-worst-computer-viruses-in-history

[8] https://arxiv.org/pdf/2204.00985.pdf

[9] https://www.mdpi.com/1999-5903/13/6/154

[10] https://www.researchgate.net/profile/Gaurav-Choudhary-8/publication/353750377$_{A}n_{A}ssistive_{T}ool_{F}or_{F}ileless_{M}alware_{D}etection/links/610e01d21ca20f6f860762cc/An-Assistive-Tool-For-Fileless-Malware-Detection.pdf$

[11] https://www.turcomat.org/index.php/turkbilmat/article/view/5620/4710

[12] https://www.mdpi.com/2071-1050/14/1/8/htm

[13] https://www.hindawi.com/journals/cin/2022/1615528/

[14] https://www.koreascience.or.kr/article/JAKO202106957226297.pdf

[15] https://www.researchgate.net/publication/338377124$_{A}Comprehensive_{R}eview_{o}n_{M}alware_{D}etection_{A}pproacheshttps://calhoun.nps.edu/bitstream/handle/10945/66993/Spectral_{G}raph-based_{C}yber_{W}orm_{D}etection.pdf?sequence=1isAllowed=y$

[16] https://iopscience.iop.org/article/10.1088/1755-1315/632/5/052065/pdf