

CYBER ATTACKS AND ITS DIFFERENT TYPES

Jibi Mariam Biju¹, Neethu Gopal², Anju J Prakash³

^{1,2}Mtech, CSE Department, Sree Buddha College of Engineering, Kerala, India

³Assistant Professor, CSE Department, Sree Buddha College of Engineering, Kerala, India

Abstract - Technology has made human life more straightforward as it brings everything to our finger tips. The invention of computers and mobile phones brought us higher attainment with time and they played a vital role in accomplishing our day to day task with ease both in professional as well as in personal lives. They are not only a simple means of gaining information and communication but also a means for data storing and data warehousing i.e we can store much important information on them. They include credit card details, passwords, user credential information etc. Most of these data are stored in plain text and can be easily obtained. Cyber criminals aim at getting the information, gaining access to information between a client and a server by spreading malware and thereby gaining unauthorized access which is known as cyber-attack. There are different types of cyber-attacks and there is a need to be aware of such attacks in order to protect ourselves from attackers. This paper provides an overview of different cyber-attacks and how it can be prevented.

Key Words: Cyber Attacks, Cyber Security, Malwares

1. INTRODUCTION

Cyberattack is a kind of attack that targets computer or computer network in an attempt to steal, alter or destroy any critical data present in it. The attacker can be any individual or a process that gain unauthorized access or use. Cyber-attack can be operated either by an individual or by groups. The aim of cyber-attack is to get the information system of an individual or a management. Cyberattack make use of malicious code and hence it changes the computer data, code or logic. This leads to disruptive effects and compromise data and lead to cybercrimes such as theft of information and identity.

2. WORKING OF CYBER ATTACK

If cyber-attack is executed by an experienced and skilled rival, it may involve many repeated pages. Hence by understanding the different kind of attacks and the stages involved in it, one could protect himself from the attack. Attacks can be grouped into two types: targeted and untargeted.

Targeted attack: In this kind of attack, the attacker has a special concern on a particular organization or has been paid to target such organization. The preparation of such attack may take long time so as to find best way to carry out the exploit to the system. The targeted attack causes more threat

than the untargeted as they are specifically made. Examples includes spear phishing, deploying a botnet, subverting the supply chain etc.

Untargeted attack: In this kind of attack, the attacker targets as many devices or users widely. Here the attacker may take the advantage of the openness of the internet. Examples include phishing, ransomware, scanning.

The different stages involved in most of the cyber-attack are survey, delivery, breach and affect.

- **Survey-** In order to determine the possible threat information about the target is analyzed.
- **Delivery-** Attending to the factor in a machine in which a vulnerability can be exploited.
- **Breach** – Exploiting the vulnerabilities to take the advantage of unauthorized access.
- **Affect** - Carrying out activities within a device that reap the attacker's goal.

3. TYPES OF CYBER ATTACK

3.1 Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks

A denial-of-service attack overruns the system resources so that it cannot answer to the service request. The host machine which are affected by malicious software that are controlled by an attacker launches DDoS attack. In this kind of cyber-attack, the machine or network resources are made unavailable for the intended user by disturbing the service of the host which is connected to the internet. TCP SYN flood attack, teardrop attack, smurf attack, ping-of-death attack and botnets are the different type of DoS and DDoS attacks.

It is very difficult to prevent DoS attack as it is very challenging to differentiate a legitimate one from a malicious traffic request as they use same port and protocol. In order to protect the system from denial-of-service attack, make sure that the system contain IDS, DDoS protection product. It is necessary to ensure that there is surplus of bandwidth internet connection on a particular organization. As there is large bandwidth for service traffic requests, it helps to protect against low-scale DDoS attacks.

3.2 Man-in-the-middle (MitM) attack

A MitM attack takes place when a third party comes in between the communication of a client and a server. The third party impersonates both the client and the server and gain access to the information between them. This kind of attack makes a threat actor to seize, send and receive the data which intended for someone else others. A MITM attack misuses the real time operation of transactions, communication or exchange of other information. The different types of man-in-the-middle attack includes session hijacking, IP spoofing and reply. An intrusion detection system can be set up in order to avoid man-in-middle attack. It helps to give immediate alert if someone tries to hijack the network flow. Virtual private network can also be used to prevent man-in-middle attack. This helps to create additional secure layers when accessing a company's confidential layer via Wi-Fi.

3.3 Phishing attacks

Phishing attack is the means of sending fraudulent emails that seems to come from trusted sources. The main goal of this kind of attack is gaining personal and credential information. Phishing attack is a form of social engineering and technical trickery. It is in the form of emails which consists of embedded hyperlinks that loads malware onto our system. Sometimes this link also leads to an illegitimate website that makes us to download malware or give up our personal information. To get sensitive data phishing attack make use of some media tools, messages, calls etc. whaling, spear phishing, pharming and deceptive are the different phishing techniques.

In order to reduce the risk of phishing attack, critical thinking, hovering over the links, analyzing email headers and sandboxing can be used. Moreover, by giving awareness among the organization employees as well as for individuals we can prevent phishing attack to some extent.

3.4 Drive-by-download attack

Drive-by-download attack is a common kind of cyber-attack carried out by the cyber criminals to spread malware and gain unauthorized access. This attack occurs when a computer becomes infected by a malicious software by simply visiting a website. The user does not need to click anywhere to get infected, that's why it is called "drive-by" download attack. Here the criminals often use a legitimate website and inject a malicious object inside the web pages. The users cannot observe the infections and range from malicious JavaScript code to iFrames, links, redirects, cross-site scripting, and other malicious elements. At the time when a user visits that infected web page, malicious codes are automatically loaded into the user's browser. Then it suddenly scans the computer security vulnerabilities in the operating system and other applications.

Updating the software quickly and regularly, removal of unwanted software applications and browser plug-in, by using firewall and web filtering software can be used to prevent drive-by download attack. Moreover, any kind of malicious software can enter itself into a system without any explicit permission when we are using a privileged account whenever to browse the internet. Such entry to the system can be prevented by keeping two separate account. One can be used for daily activities and other can be used for administrator account for installing software.

3.5 Password Attack

The most common method to authenticate user is to use passwords and obtaining such passwords is an effective attack approach. Password attack is the technique in which user's password is obtained or decrypted by illegitimate means. User password can be obtained by looking around the user's desk, by guessing, accessing password database, sniffing the network connection to get the plaintext password etc. Password sniffers, dictionary attacks, cracking programs are the different methods used by the cyber criminals in password attack. By changing the passwords frequently, using unrecognizable words and minimum length can the different means by which password attack can be defended. Brute force and dictionary attack are the two main techniques in which password can be obtained. Brute force is a random method in which different passwords are tried expecting that one password will work whereas the later method gain access to a user's computer and network.

3.6 SQL Injection Attack

SQL (Structured Query Language) is a computer language that is used to store, manipulate and retrieve data stored in the database. SQL language uses commands like select, update, delete to perform the required task. SQL can also execute queries against the database, insert records to the database and can create new tables in the database. SQL Injection (SQI) attack make use of malicious code in order to access information by manipulating database at the backend. This information may include any sensitive organization details, customer/ user private data etc. This may result in the illegal viewing of the user data, deletion of the table data and unauthorized attack of database.

An attacker who wants to execute SQL injection will manipulate a standard SQL query to exploit vulnerabilities in a database that are not validated. Attackers can also use mis-filtered characters to alter SQL commands. There are several effective ways to prevent and protect against SQLI attacks if they occur. Input validation can be performed to identify unlawful user inputs which is the writing code practice that can. But this method is not much suitable as the mapping of all legal and illegal inputs is not feasible. Because of this, usually a web application firewall (WAF) is used to remove out SQLI. Signature recognition, IP reputation and other

security methods can also be used to identify and block SQL injections with a minimum of false positives.

3.7 Cross-site scripting (XSS) attack

Cross-site scripting is a common type of injection attack that inserts malicious code into a trusted web site or into a sensitive web application. In other words, XSS occurs when the attacker injects a malicious code or JavaScript into website's database. The intruder injects malicious JavaScript code into the end user's webpage and make him/her to download the webpage. The browser of the victim executes the malicious script within the response, sending the cookies of the victim to the server of the attacker. There are three main types of XSS attack: Persistent XSS, Reflected XSS and DOM based XSS. In persistent XSS, malicious code arose from the website's database whereas in case of Reflected XSS, malicious code arose from the victim's request. DOM based XSS is an alternate for above mentioned methods. Here the vulnerability is present in the client side not in the server side. Cross-site scripting can be prevented either by encoding or validation. Encoding escapes the user input so that the browser interprets it only as data, not as code and validation filters the user input to be interpreted by the browser as code without malicious commands.

3.8 Eavesdropping attack

Also known as sniffing or snooping attack. Eavesdropping attack deals hacking data that are sent through digital devices. Attacker uses insecure network for communication and examines send and receive data. As they do not show any abnormal operation during transmission via network, this kind of attack are very hard to detect. Using this method an attacker can obtain various information like credit card number, password and other sensitive information that are sent across the network. Attacker may introduce sniffer on a computer or server to perform the eavesdropping attack seize data during transmission. This attack can be of two types: Passive Eavesdropping and Active Eavesdropping. Passive Eavesdropping takes place by listening to the message transmission in the network, attacker uncovers the data. In Active Eavesdropping, attacker get the data by pretending himself as a friendly unit and sending transmitter queries. Use of an anti-virus software, firewall, virtual private network, encryption and avoiding the public network for transmitting sensitive data helps to prevent eavesdropping attack.

3.9 Birthday Attack

Birthday attack is a kind of cryptographic attack belonging to a brute force attack class. It works on the principle of birthday problem in probability theory. This attack can be used to misuse the exchange of information between more than two parties. Birthday attacks are carried out using hash algorithms to check the message integrity, software or digital

signature. Hash function processed message produces a message digest of fixed length. This message digest exclusively defines the input message as it is independent of the length of the input message. Birthday attack is the process of finding two arbitrary message that generate same message digest when processed by a hash function. If the sender calculated message digest is same as that of the message digest calculated by an attacker, the attacker can replace the message of sender with attacker message. Thereby the receiver of the message cannot recognize the message as fraud as it shows same message digest.

3.10 Malware Attack

Malware attack is a class of cyberattack in which malicious software is installed into the user's computer without any consent of the user. This is what we called now as virus, spyware or ransomware etc. Malicious code is attached to the legitimate code, get propagated and executed by themselves. Malwares are able to access private network, interrupt certain computing operation, steal sensitive information or any other user data and thereby making money illicitly from the target. Now a day, malware aims more at business or financial information than any credential personal information. Most common type of malware includes:

- Virus: A malicious software that get attached to any computer program, replicate and modify codes when executed. It can spread either by downloading a file or running any program.
- Worms: spread across computers or networks via email attachments. This may result in denial-of-service attacks
- Trojans: One of the most danger malware which has malicious function. It hides in a useful program and do not replicate like viruses.
- Ransomware: A type of malicious software that locks out the user data and threatens user unless a ransom is paid. It is very difficult to prevent this attack even though the code is simple.
- Spyware: A kind of malware that inspects the user activity without user approval and report it to the attacker.

4. CONCLUSION




Cyberattacks are one of the most ambiguous factors which is quickly and constantly evolving that causes threat to computer or computer networks. Cyber criminals have introduced different hacking techniques and causes individual as well as business sectors more vulnerable to security problems. This paper outlined about the most common cyberattacks that are used by the attackers in order to compromise our critical information. These attacks cause a negative impact on the integrity, confidentiality and

security of the system as well as the network. The major thing that we can do is to protect ourselves from attack is to understand about the possible threat and take required steps to safeguard the system and network.

REFERENCES

- [1] Cyber-Attacks-Different types and its prevention methods, <https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html>
- [2] Top 10 common cyber-attacks and it's counter measures <https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks.html>
- [3] Andreea Bendovschi, "Cyber-attacks – trends, patterns and security countermeasures" in ResearchGate, 2016.
- [4] Antesar M.Shabut," Cyber Attacks, Countermeasures, and Protection Schemes–AState of the Art Survey", 2016 10th International Conference on Software, Knowledge, Information Management & Applications.
- [5] L. Meyer ; W.T. Penzhorn "Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks", IEEE AFRICON 2004
- [6] Oliver Eigner "Detection of Man-in-the-Middle Attacks on Industrial Control Network", 2016 International Conference on Software Security and Assurance <https://www.veracode.com/security/man-middle-attack.html>
- [7] Tommy Chin, Member, IEEE, Kaiqi Xiong, Senior Member, IEEE, and Chengbin Hu, "PhishLimiter: A Phishing Detection.
- [8] Aditya K. Sood," Drive-By Download Attacks A Comparative Study", IEEE Computer Society,2016
- [9] Hong-Ning Dai ; Hao Wang ; Hong Xiao ; Xuran Li ; Qiu Wang, "On Eavesdropping Attacks in Wireless Network"
- [10] Rahul Raveendranath ; Venkiteswaran Rajamani ; Anoop Joseph Babu ; Soumya Kanti Datta, "Android malware attacks and countermeasures: Current and future directions"

BIOGRAPHIES

	<p>Jibi Mariam Biju, she is currently pursuing M.tech in Computer Science and Engineering in Sree Buddha College of Engineering, Elavumthitta. Her research areas include the field of data mining, cryptography and security.</p>
	<p>Anju J Prakash is working as Asst.Professor in computer science and engineering in Sree Buddha College of engineering, meanwhile pursuing her PhD in the field of image processing or data mining from Noorul Islam Centre for higher education.</p>
	<p>Neethu Gopal, she is currently pursuing Master's Degree in Computer Science and Engineering in Sree Buddha College of Engineering, Elavumthitta, Kerala, India. Her research area of interest includes the field of Security and Blockchain Technology.</p>