On Cybersecurity Attacks

It covers cybersecurity attacks and their types.

Ümmü Gülsüm Varlı

Table of contents

Cybersecurity Attacks:

1. What Is a Cybersecurity Attack?

Cyber Security attack is the method of attacking one or more machines, opening a war, corrupting their data, stealing their data or all the slightest changes made on it. Cybersecurity attacks are a comprehensive discipline that is very diverse and classified. Even if you are on machines that you believe to be very secure, a cybersecurity attack is always available to be tried, successful or unsuccessful. It is available in the open wherever the system is. Cyber security attacks are also the use of vulnerabilities in systems, finding and attacking them with various tools, methods, malicious software. We must not forget that potential goals are always present and will continue to exist.

So what are these types of cybersecurity attacks and can't we be protected from them?

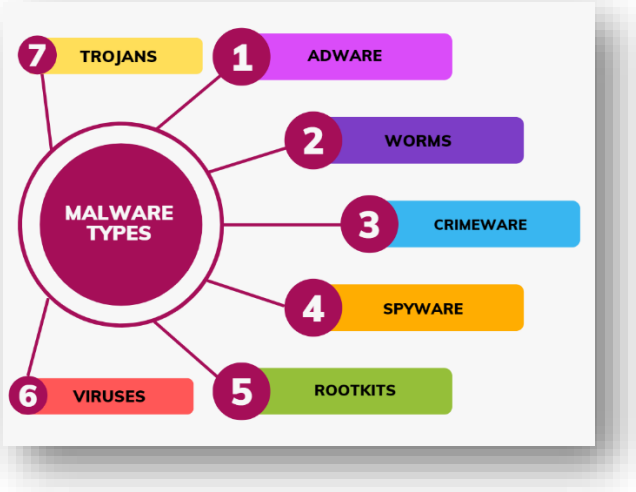
Of course, there are many types of attacks and methods of protection.

2. Types of Cyber Security Attacks:

Although the types of cyber security attacks are very diverse, when it is tried to list the most important ones as *Malware (malware), Phishing*, *DDoS and DoS*, *SQL Injection*, Cryptojacking, Password Attacks , Supply Chain Attack, *Eavesdropping Attack*, *Zero Day Exploit,* Man in the Middle.

2.1. Malware:

It is the type known as the most malware worldwide. It is a kind of successful enough in infiltrating your electronic devices with different infiltration methods to neutralize the devices or to neutralize you. Whether through advertising, through files or links, through self-replication and disabling your device, or through all your private information can seriously endanger you. Therefore, *malware* is one of the types of software that should definitely be avoided.



2.1.1. Adware Software*:*

It is defined as adware that actively runs in the background by infiltrating through computers or mobile devices where the attacker should or should not enter without authorization from the user. Adware software is not considered a virus because it can only actively process on the machine on which it is installed. It is a type of malware that can work in the background and install heavy damage on the system. It can be transmitted through web pages or free software downloads. For this reason, it is recommended that you do not download anything from sites that you do not trust.

Choosing reliable websites to protect yourself from adware software and using anti-virus software on the devices you use will help protect you.

2.1.2. Worms:

Unlike viruses, worms are a type of malware that can copy and reproduce itself. Worms are used to copy from one computer to another. Worms can spread very quickly in a very short time without the need for any action. Similar to a DDoS attack, this slows down traffic and can render your device nonfunctional. Servers may not be able to handle this traffic, which makes the system ineffective. Worms can often be transmitted through e-mail or from untrusted, obscure sites.

For example, if we refer to the examples of worms on the Internet;

- Congratulations! You are entitled to a free visa to America.
- You are the 10,000th person to enter our site, so we give you an iPhone as a gift.

Usually, there are worms in the links to your social media accounts and when you click on these links, they send them to the URL or IP address in the background and from there they can seize your information or make money on you.

2.1.3. Crimeware:

Crimeware is software designed to automate cybercrime. It is mostly malicious software used by people who are interested in social engineering. It can undermine network security, hijack your data, and give you huge losses by gaining access to your bank accounts. It can provide remote access to networks that should not be entered for malicious purposes, access and change your sensitive data, blackmail by demanding a ransom payment, so it is one of the types of malware that should be seriously considered.

To protect yourself from such situations, you can install security software, add security patches to your operating system, and read and approve personal text on sites.

2.1.4. Spyware:

Spyware is one of the most annoying malware for companies, institutions-organizations. Spyware can secretly collect data from your devices. They can save passwords on your computer, take screenshots. In addition, these software are not only limited to Windows, but can also infiltrate your Mac computers. They can offer poor service by hacking your site and making it closed. They can leak user data, leaving much greater damage. In fact, there is nothing strong yet at the point of protection because there are so many potential spyware tools available and the potential is more than minimal. So always keep your data redundantly somewhere.

2.1.5. Rootkits:

Root comes from Linux and Unix, which have "privileged control system privileges", while the kit meets the meaning of "administrator-level access". So they can have everything, they can access data by accessing networks, they can start a DDoS outbreak.

The root user definition, as the name suggests, tries to live on a device by hiding it by pretending to exist at the root of something. Its purpose is not to copy or reproduce itself, but to be able to live in a hidden way on the device it is on. It is one of the most powerful types of malware. They can reach all the way to the system kernel and patch themselves.

In addition, since it can reach the system core, it is not only content with the collapse in terms of software data, but also leaves hardware damage. Documents, files, links that you are not sure of the source of can infect rootkits. Those who are on the hunt for social engineering can use rootkit software to gain access to your credentials, so organizations need to regularly monitor penetration testing on everything they use.

There are 3 types of rootkits . These can be sequenced as kernel, bootloader, and memory.

a) Kernel: Reaches the core of your computer and changes the functioning and working order of your operating system.
b) Bootloader: The bootloader rootkit loads a fake operating system before the bootloader and then replaces it with the normal operating system. In this way, it becomes active and takes over the operating system.
c) Memory: It cannot be permanently located on the computer because it tries to be located in the RAM region of the computer and not in the ROM (permanent region) of the computer. It will be deleted in ROM memory. It decreases the performance of the computer because it runs in the ROM zone in the background of the computer, but when the computer restarts, the ROM will disappear because it refreshes itself.

2.1.6. Viruses:

It can be said that it is malicious software programming that is stored by accessing the device without user permission, changing the way it works. For malware to be in the category of viruses, it must be able to self-replicate and run itself.

If we try to categorize viruses among themselves, they can be divided into macro-viruses, file-viruses, network-viruses, software bombs, xss/cross site scripting viruses in terms of their importance.

- Macro-viruses can be found in places that contain macro programs. Like Office programs.
- File-viruses are viruses that activate and run when they are held and run as hosts to executable files.
- Network-viruses first try to infiltrate the network and then try to infiltrate potential targets. They can quickly spread on the Internet, in local networks.
- Software-bombs are activated and activated in the appropriate environment when the necessary conditions are created according to the coding.

2.1.7. Trojan:

Trojans can delete, block, modify, copy data, reduce the performance of devices. They can not multiply on their own, they can not be treated on their own. They wait to be started by an attacker or a user. A Trojan horse is a computer program that installs malware.

One of the simplest examples is the program called "Waterfalls.scr". When this program is executed, the trojan horse becomes active. The program promises to give you a free screen saver when you install it in the first place.

Trojans are classified according to how they can damage the system. When classification is provided in this way, 7 main types of trojan horses appear.

1. Remote Access
2. Email Sending – Sending emails
3. Data destruction
4. Proxy Trojan – Proxy Trojan: Hides the infected system in the malware.
5. Ftp Trojan – Ftp Trojan: Performs the process of attaching or capturing files from a malicious computer.
6. Disable security software
7. DDoSS Attacks
8. URL Trojan – They are classified as URL Trojan.

2.1.7.1. What can these trojans do with these attacks?

- They can encrypt files with the method of "cryptoviral extortion".
- They can damage files as well as encrypt them.
- They can delete and overwrite data.
- They can hijack the computer camera and take a picture of the user.
- The user can gain remote access to the computer. (RAT- Remote Access Trojan)
- They can damage your firewall, disable it.
- They may collect emails to send spam emails.
- They can save and steal your passwords with the "keylogger" method.
- They can work on memory in a hidden way.

2.1.7.2. Ways to protect yourself from a Trojan Horse:

- Do not use programs that share a local network.
- Scan your emails from someone you don't know before opening them. Investigate the sender's source of the sender sent it.
- Have an anti-virus program on your computer. Stay up-to-date.
- Operating systems provide updates by taking viruses into account in the updates that come to computers. So keep an eye on your operating system updates.

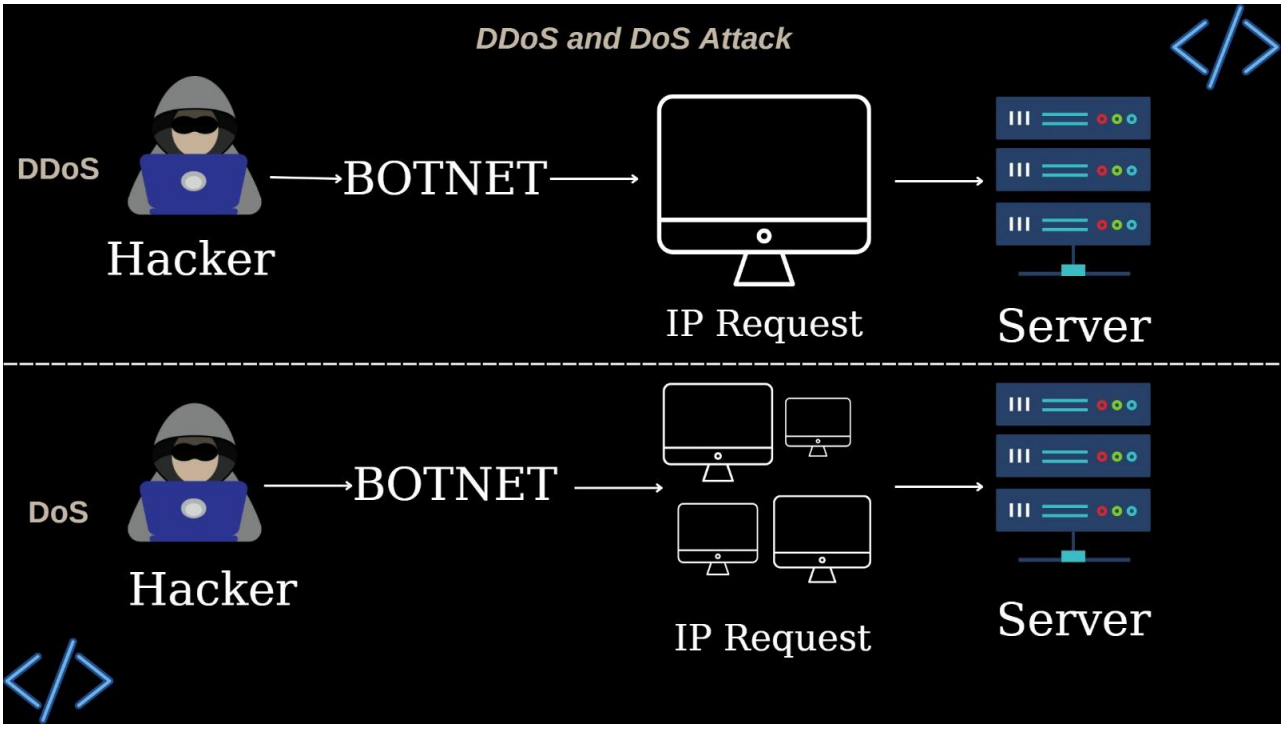
Trojans are often infected with fraudulent programs. Therefore, it is recommended not to open anything unfamiliar. Because there may be a worm or trojan horse in an image, link and the program is activated as soon as you open it.

2.2. Phishing:

Although the sensations of phishing attacks have become very widespread, they can still be described as the biggest enemy of those who do not know. In general, the method of infiltration in a phishing attack is very simple and classic. E-pos takes what is asked of you by making you believe what it wants to believe through t a or link. Therefore, attention should be paid to what comes to e-mails and information should be obtained about official e-mails so that e-mail separation can be made easily. Since it is almost the oldest known method of attack, people are now more aware of this attack than in the past.

2.3. DDoS and DoS:

The cybercriminal sets up a "*zombie network*" of computers, usually spreading viruses, to send many requests to the potential target. It sends too many requests to the server, pushing traffic and preventing the systems from working. It aims to disrupt or stop the services offered by the computer connected to the Internet. It is one of the most common types of cyber attacks from past to present. DoS is called decommissioning. It sends too many requests to running services, the server fails to withstand this traffic and goes down. DDoS consumes distributed service servers unexpectedly. It sends almost thousands of IPs in seconds, blocking system access. DDoS is a type of attack prepared by hackers. They do it with botnet networks. They ensure that serious deficits are given on the servers.



Slowing down the system speed compared to normal, having too much network traffic, too many UDP, SYN and GET/POST protocol requests are signs of a DoS or DDoS attack.

They are known in the Internet world as almost the oldest and most effective types of attacks. Since it was created by attackers, the exact solution has still not been determined.

2.3.1. DoS and DDoS Types:

- Volume Based DDoS (Volume Based Attacks): In the computer world, each server has bandwidth. Thanks to these bandwidths, the capacity of the server is obvious. If requests are sent to the server beyond its capacity, the server cannot remove it and it becomes disabled, unable to respond to requests. That's what this attack is aiming for. More requests are sent to the server than bandwidth can handle, and the server cannot respond to incoming requests.
- Protocol Based DDoS (Protocol Based Attacks): There are protocols that are actively used in the use of the Internet, and the operation is provided according to these protocols. OSI (Open Systems Inter Connection) protocol is one of them. Protocol-oriented attacks are attacks that target OSI layers. Located in OSI, the 3. (network layer) and 4th layer (transport layer) protocols. The fact that the protocols have been used for years and have not been updated makes these attacks powerful and effective.

- Application Layer DDoS (Application Layer Attacks): The application layer, which is the 7th layer of the OSI protocol, is utilized. In this type of attack, GET and POST properties are used from HTTP methods in data packets by exploiting service vulnerabilities at the application layer. GET and POST methods are tried to consume the system with network traffic. With the GET method,the resources on the server are accessed and the data is sent to the server with the POST method. With the data density in the servers, it is ensured that the servers cannot respond.
- UDP Flood DDoS Attacks: A type of DDOS that is made using vulnerabilities in the UDP protocol. UDP packets are sent to the server excessively, making the UDP Ports unusable, making the server unresponsive.
- PING Flood DDoS Attacks: In PING Flood DDoS attacks, PING packets are used and a traffic network is created, aimed at increasing the consumption of the server. When the server tries to respond to the PING packets sent, CPU and RAM consumption is ensured and it is not responding. In general, these attacks using protocol vulnerabilities are successful. This provides companies with a high rate of financial loss. In order to minimize this, enterprise-organizations should have different types of test infrastructures against DDoS attacks or receive this service. At the same time, large companies can also have these tests done.

In terms of businesses, there are many points of DDoS vulnerability in their network infrastructures, ranging from configuration errors, bandwidths and applications used. The people who will perform these tests and those who are responsible for protecting your organization should also technically be specialized in protocols such as TCP/IP. (berqnet)

2.3.2. DoS and DDoS Attack Prevention Methods:

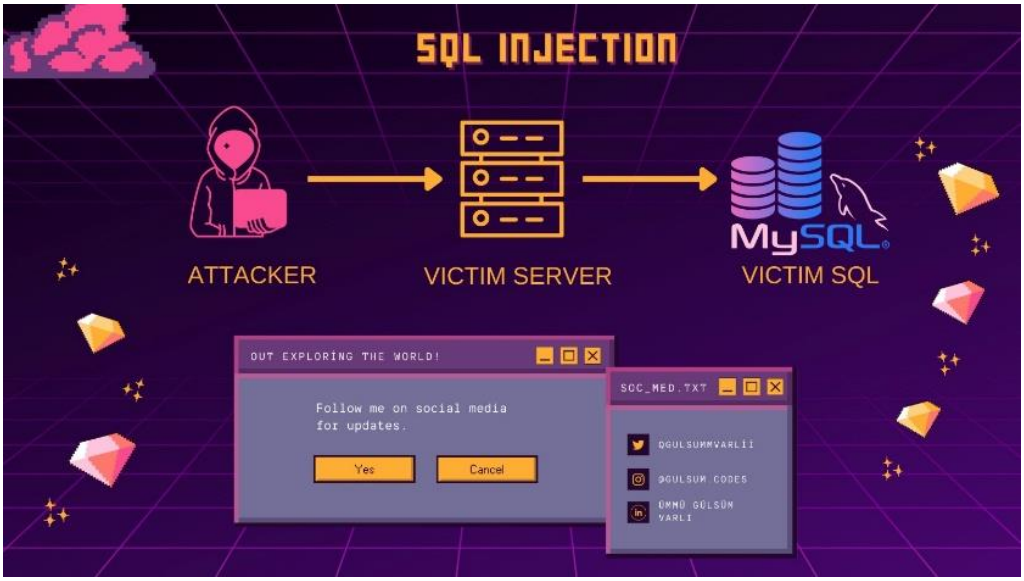
As a matter of fact, it is very possible to make a DDoS attack and be successful today. Therefore, companies should regularly undergo the testing process.

- Use a firewall or anti-virus.
- Make system updatesin a timely manner.
- Network traffic should be monitored, network devices should be configured for unusual situations. For routers, methods such as rate limiting, blocking of fraudulent and corrupted packets, and determining the threshold values of SYN, ICMP and UDP packets can be applied.
- The bandwidth should be more than the institution needs.
- For large-scale enterprises, Content Delivery Network (CDN) can be used to store data on multiple servers around the world.

2.4. SQL Injection:

SQL stands for Structured Query Language . SQL is a sub-language used to manage and design data. Almost everything that has data in it has SQL in its infrastructure. Therefore, companies that have data are very likely to be attacked by this attack. SQL injection is one of the most widely used web hacking attacks and is one of the code injection techniques that can destroy a database.

SQL injection typically occurs when you request input from a user, such as username/user ID, and instead of name/identity, the user gives you an SQL statement that you will unknowingly run in your database.

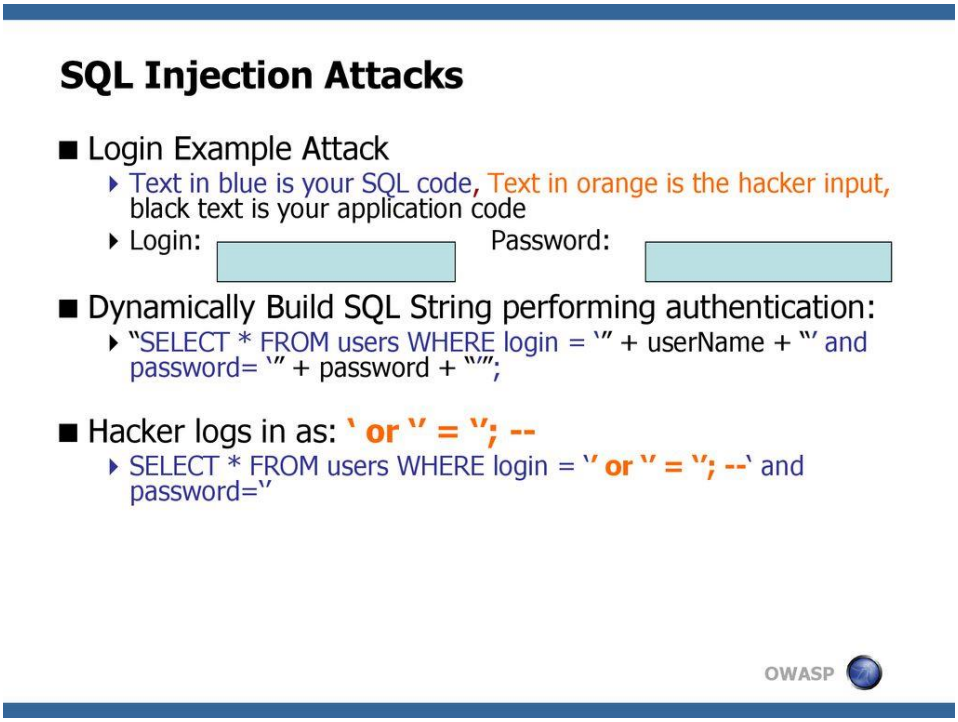


See the following example, which creates a statement by adding a variable (txtUserId) to the select string.

- Variable fetched from user input (getRequestString): SELECT
- Example
- txtUserId=getRequestString("UserId");txtSQL="SELECT * FROM Users WHERE UserId=" + txtUserId; (w3school)

SQL: It helps to pull and process data from databases such as MySQL, MSSQL, Oracle, allowing us to obtain information about the data in these data tables. The fact that we can collect the data and change it at any time makes this sub-language popular.

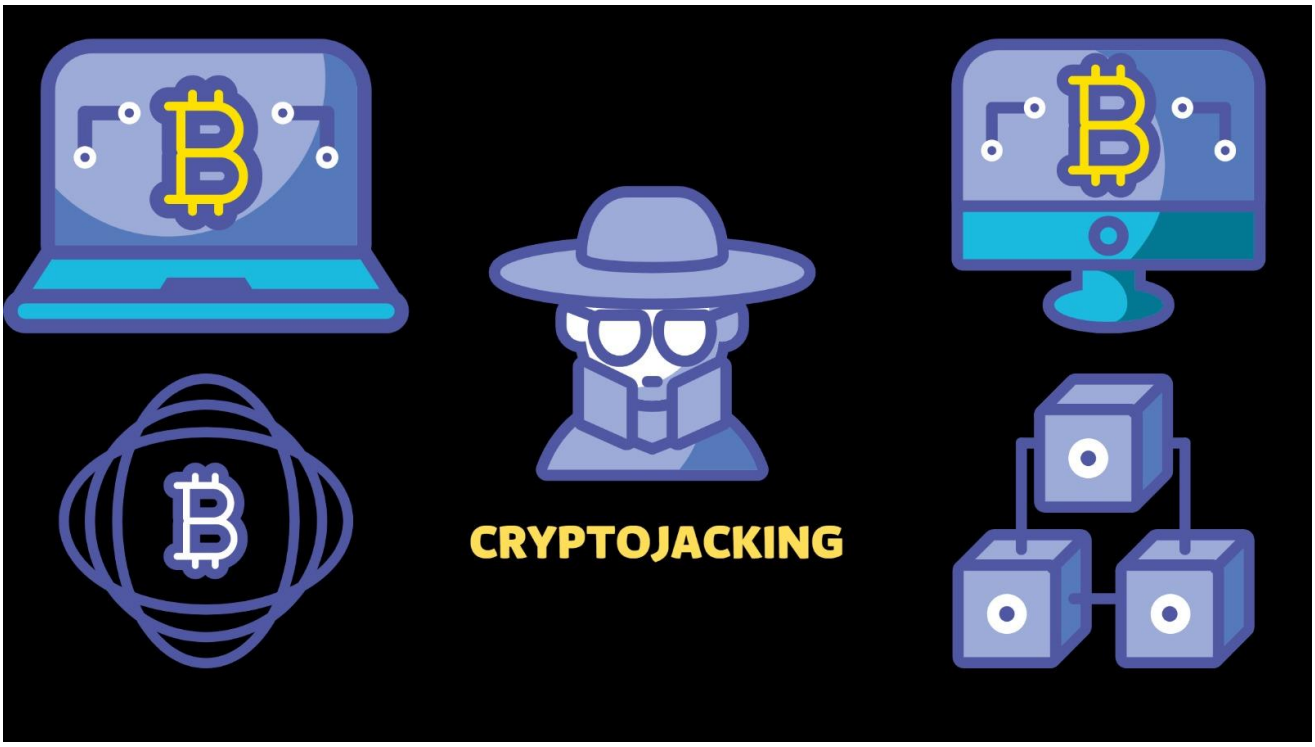
SQL is when the web application intercepts the SQL query it makes, gaining unauthorized access to the data in the database. When logged in to any application, the user can only see his own data. However, in SQL injection, the attacker can also access the data of other users.



This vulnerability, which we encounter in web-based applications, is used for data theft. When filling out a form on a website, a SQL query is sent to the background, communication with the database is provided. This channel can be manipulated with a different SQL query in a fraudulent way and the whole database can be hijacked. The SQL injection method is effective on forms available on your websites. That's why you shouldn't neglect the security of your pages. The slightest vulnerability can lead to huge data breaches for the company.

2.5. Cryptojacking:

Cryptojacking, that is, the process of entering unauthorized places of the computer for the purpose of mining crypto money. Attackers can attack with ransomware, unreliable websites, or unknown email. Thanks to the fake email, crypto mining codes can be installed. In this way, it can also access the computersof the victim and infect the scans or website contents. This uses the computer's processing power and other resources in the background while users continue to browse normally.



Cryptojacking can be done by multiple methods and can run in the background, consuming the computer and damaging its operation. The most common of these attacks are using phishing methods to convince users to click on links, injecting malware, scripts and advertisements that redirect to websites. The purpose of cryptojacking attacks is to gain access to the CPU (Central Processing Unit) system. Because the CPU is where computers process data and perform software commands, those who suspect this attack should first evaluate the computer's operating performance.

2.5.1. Examples of Attacks:

- With **FacexWorm**, one of the malicious Google Chrome extensions discovered in 2017, it is possible for users to access their computers with the Facebook application.
- Encrypted malware on Github, where open-source code, one of the largest platforms worldwide, is stored , facilitates resource access.

2.5.2. How is Cryptojacking Detected?

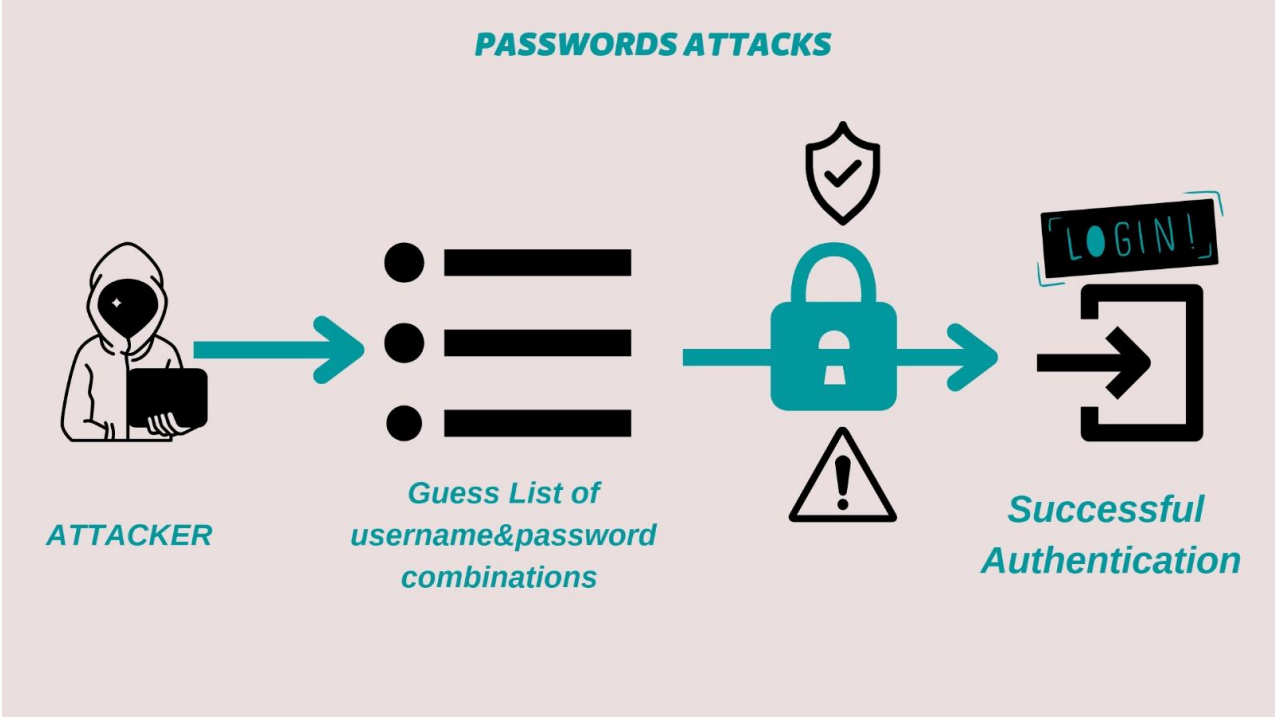
- While these attacks take place in the background, they will cause performance degradation.
- Staff who experience slowness at the computer should first look at the help desk. Therefore, the person who examines the computer must master the cryptojacking attack.
- Attacks can be detected by network monitoring. Monitoring, analysis and management of networks enables to identify solutions designed using artificial intelligence.

2.5.3. How to Protect Yourself from Crytojacking Attacks?

- Network traffic and system traffic should be checked.
- You can use special, secure extensions from web browsers. (Anti Miner, minerBlock)
- They can be transmitted through advertising, so ad blockers like Ad Blocker can be used. In addition, reliable websites should be browsed, unknown ads should not be clicked on.
- This attack is usually designed through JavaScript code. When you suspect an attack, they can disable the JS code in the web browser and re-evaluate other performance values.

2.6. Password Attacks:

A type of attack is made to exploit the credentials of user accounts. A phishing attack, one of the most common types of attacks, accounted for more than 81% of data breaches in 2020. Password attacks aim to exploit vulnerabilities with tools that speed up the guessing or hashing of passwords.



2.6.1. Types of Password Attacks:

2.6.1.1. Phishing Attack:

It is one of the most common types of password attacks. It is the technique by which the hacker disguises himself as a trusted site by sending a malicious link to the victim. Once legitimately authenticated, the victim clicks the link to send credentials to the attacker. In phishing attacks, various methods are tried to get the user to click the link.

- DNS-cache poisoning: Attackers are redirected to a different site, similar to user requests. This means that kexploits vulnerabilities in the DNS server to convince the user.
- URL-hijacking/typo-making: Attackers create a real-looking URL that differs slightly from the site the user wants to go to. When the user makes a typo, they redirect you to the malicious page.
- Tabnabbing: They rewrite malicious sites that look like legitimate web pages.
- UI fix/iFrame overlay: Attackers add malware to a legitimate click link.
- Phishing cloning: An attack in which links in the original email are replaced with URLs of malicious sites.

2.6.1.2. Brute-Force Cipher Attacks:

Trial-and-error is used to guess the user's credentials. The attacker uses scripts to work with too many permutations. Although this method is an old method, it is used as a standard because they are automatic and simple.

2.6.1.3. Dictionary Password Attacks:

The list that is most likely to be used as a password by a particular network is generated. This predefined list consists of the user's behavior patterns and previous data breaches. These lists are passed to the automatically authenticated tool based on their user name.

2.6.1.4. Password Spray Attack:

The hackertries to authenticate using the same password without switching to another password. Password spraying is one of the most effective methods because website users set simple passwords and use the same password on several accounts.

2.6.1.5. Keylogging:

An attacker would install tools to monitor the user's computer. The keylogger records all the information that users type into their login forms and then sends it to the third party. This allows unauthorized access.

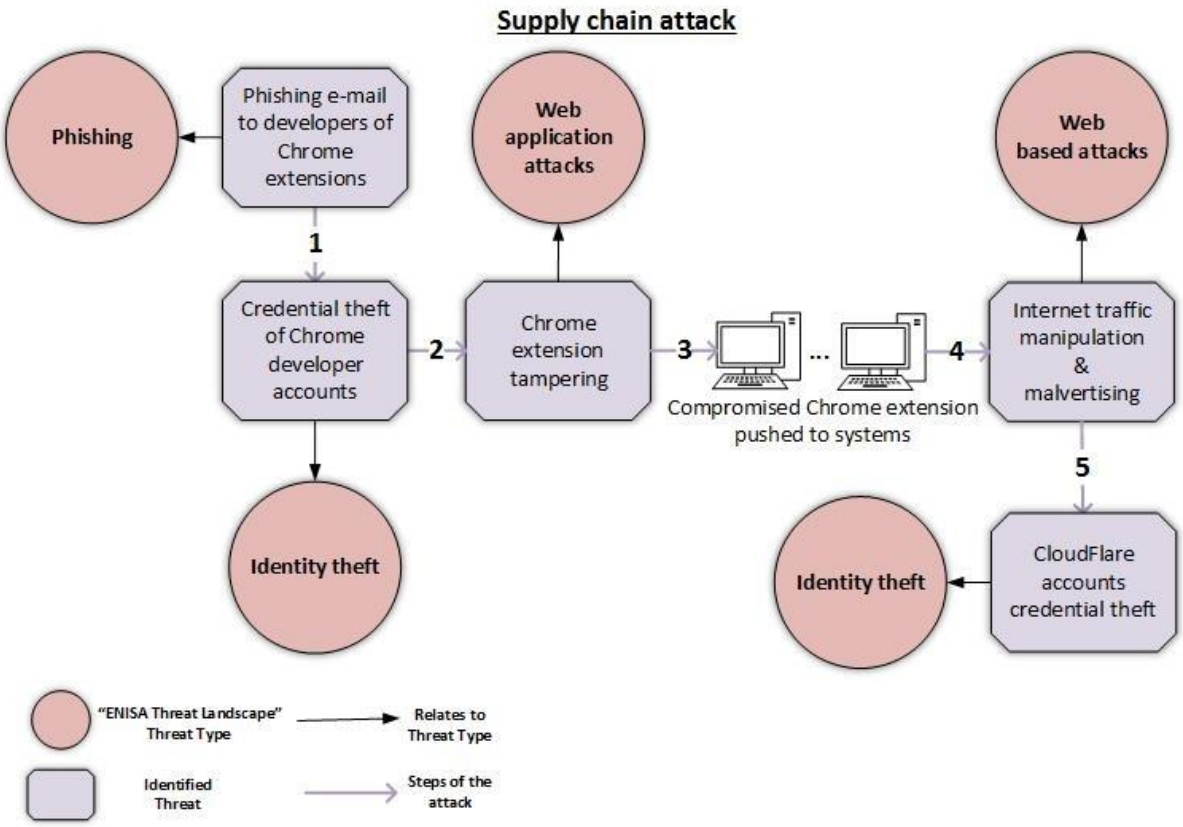
2.7. Supply Chain Attack:

Supply chain is the whole of the business models and processes that provide the integration of the basic business processes within the chain. It provides money, information and material transportation to the customer at the right time and in the right place without any problems.

Supply chain attack is called attacks that damage the operation by taking advantage of hardware and software vulnerabilities provided by institutions and organizations.

2.7.1. Types of supply chain attacks:

- Software Supply Chain Attacks: These are attacks on software used by large companies to ensure maximum workflow efficiency.
- Supply Chain Attacks Through Hardware: The supply chain attack method, which is a simple and inexpensive attack method through hardware, is realized by placing video or sound recorder devices thanks to the chips method that offers different possibilities such as USB driver or ethernet cable.
- Supply Chain Attacks via Firmware: The most preferred type of attack. More knowledge requires skills than other types. Firewalls are bypassed and systems are damaged.

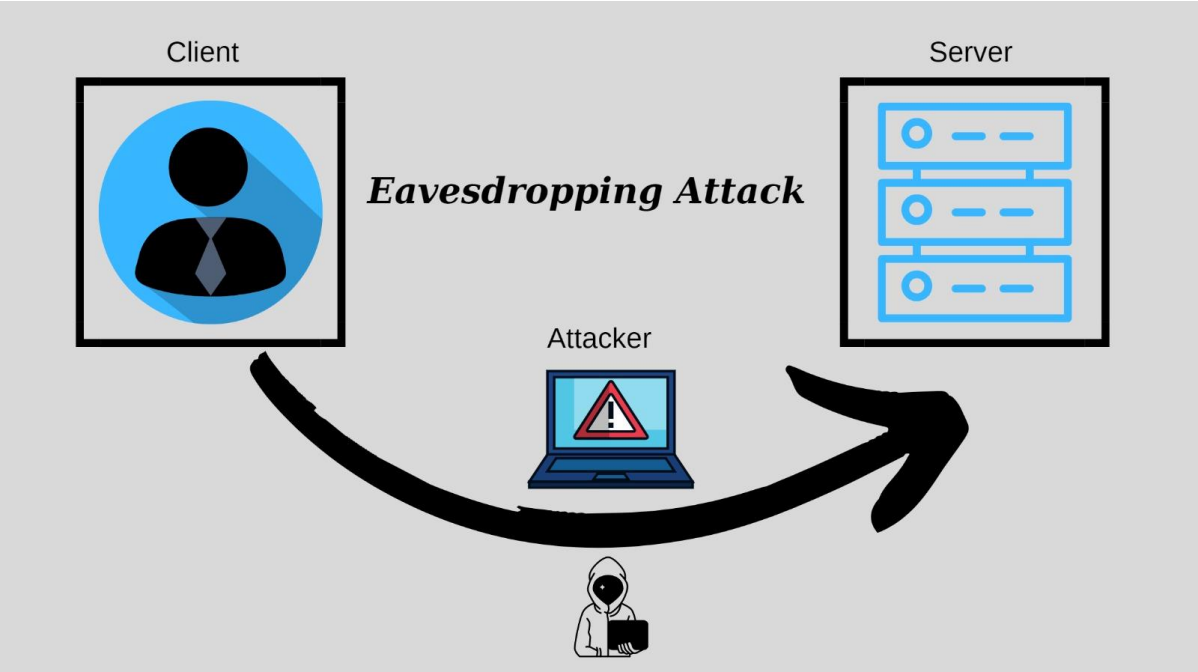


http://bit-sentinel.com

2.8. Eavesdropping Attack:

Eavesdropping, which means "eavesdropping", refers to the listening, interception or unauthorized use of data transmitted between devices by a third party in today's world.

This type of attack is now carried out on unsecured networks. That is, it is the capture of data transmitted through unsecured network connections of devices.



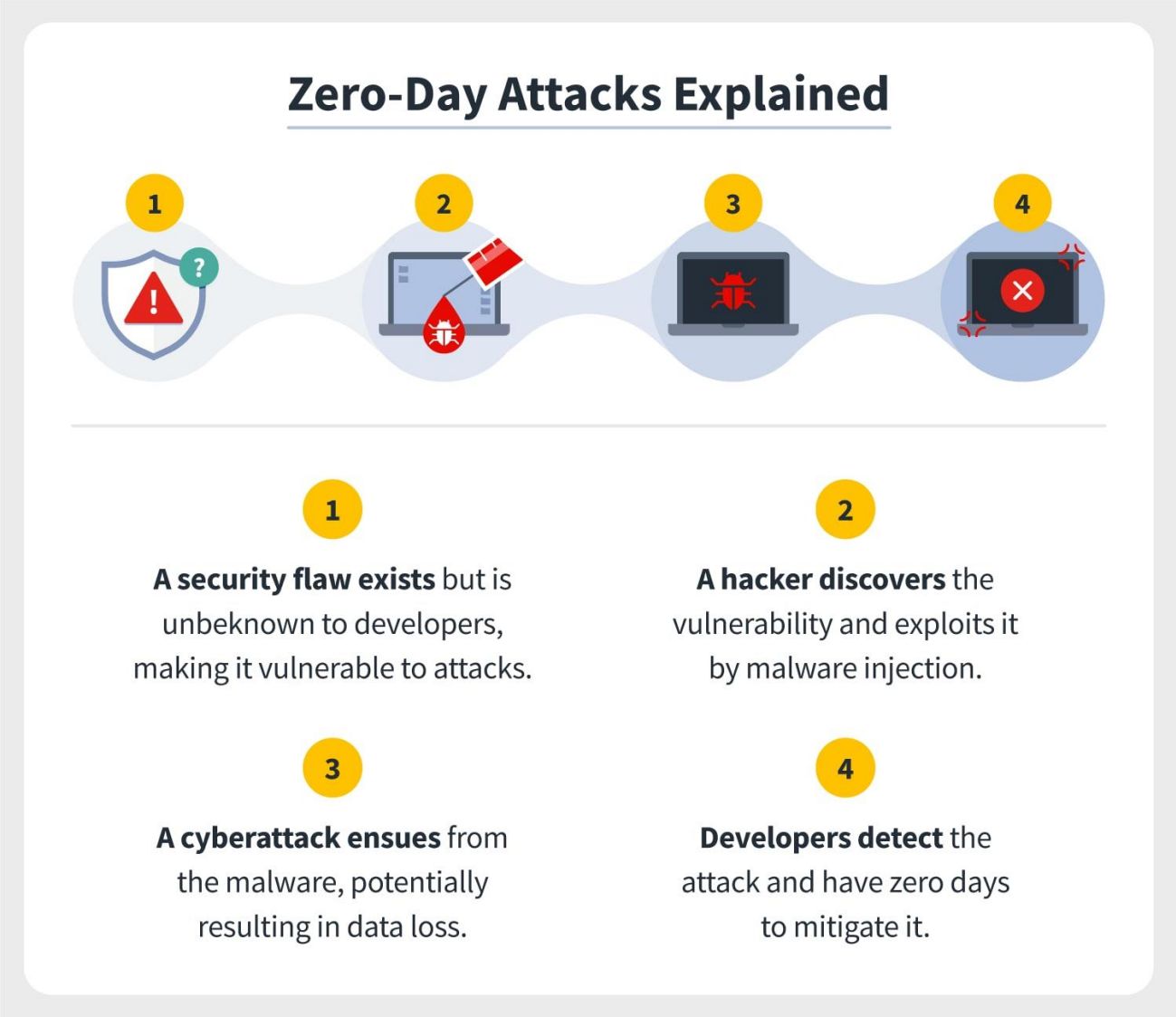
2.8.1. Eavesdropping Attack Methods:

- Passive Eavesdropping: This method is more of a passively targeted attack method to collect information. An attacker can passively monitor everything you do, collect information, but not change your data. This attack method often causes problems with public wifi connections.
- Active Eavesdropping: They can infiltrate your system over the network and modify your data . The attacker can do everything according to his own wishes.

The email you think is from someone you know and may have been sent by a third party and may be cheating on you. Hackers can copy and spoof secure IP addresses and modify trusted emails to try to reach you.

2.9. Zero Day Exploit:

It is to attack by discovering the vulnerability in the network or hardware in the place to be attacked before the developer, manager and authority of the area. The reason why there is a zero-day deficit is that it is attacked within zero days after the deficit is noticed. Once developers notice the vulnerability, they will try to patch or fix it, but it will take time. That's why zero-day vulnerability attacks are generally successful.



- **A zero-day vulnerability is when** hackers notice the vulnerability before the supplier.
- **A zero-day exploit is a** method of attack by attackers on systems that are exposed to a previously unknown vulnerability.
- **A zero-day attack is** when hackers perform an attack within zero days from the moment they realize the vulnerability.

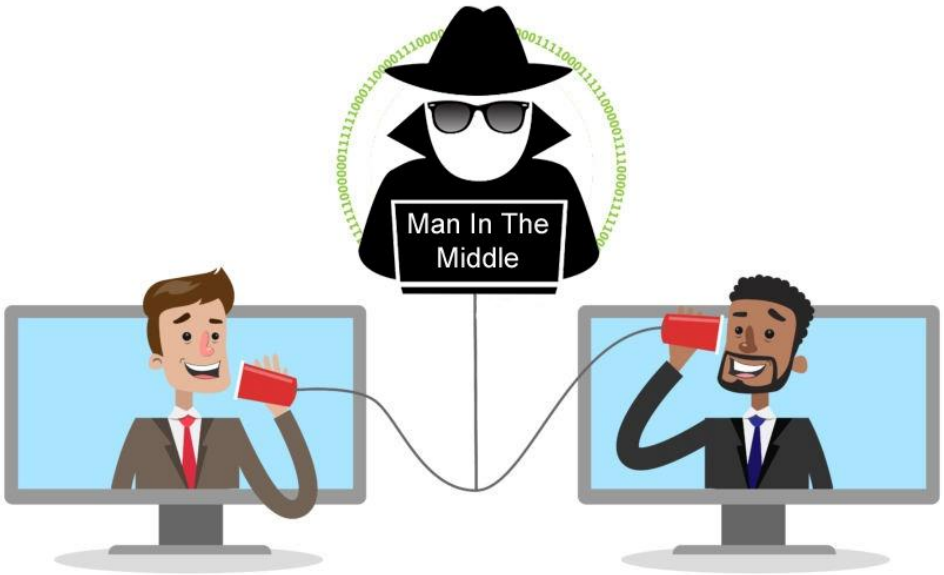
Some attackers or hackers discover vulnerabilities in the supply chain without the software developers noticing. They then write code and go on the offensive to exploit the vulnerability of this vulnerability. This written code is called "exploit code". Attackers now need access to the vulnerable system. For this, they try to access it via e-mail, which is usually one of the social engineering tricks.

The data obtained can be sold on the dark-web, and the data can be blackmailed using it. Once the exploit is discovered and patched, this threat is eliminated.

Zero-day attacks can be carried out by cybercriminals, hacktivists, cyber warriors or corporate espionage.

2.10. Man-in-the-Middle Attack:

It is a type of attack in which attackers who take advantage of weak-based web protocols access assets in an intermediary channel themselves for data theft and distort information about the data in their favor.



2.10.1.Types of Man-in-the-Middle (MITM) Attacks:

- IP Spoofing: An attacker's attempt to steer the victim's information by directing them to the seemingly legitimate site. The attacker tampered with the secure website with a fake IP.
- ARP Cache Poisoning: Address Resolution Protocol (ARP) is the protocol that is associated with a specific internet layer address and allows communication with another link layer address. ARP is important because it translates the link layer address to an internet protocol (IP) address on the local network. The victim's computer is tricked with false information from the criminal, the fraudster's computer is perceived as a gateway. Then, after the victim's computer is connected to the network, it sends all network traffic to the malicious third party instead of a real gateway. Data theft of personal information stored on the computer is committed.

- Email Interception: Cybercriminals intercept the emails of banks that have access to sensitive data or money, and the communication between the bank and its customers is provided and monitored. To make matters worse, the attacker can launder money by asking for money from the bank's customers by spoofing the victim bank's email address.
- DNS Spoofing: Domain name system (DNS) spoofing or poisoning directs legitimate traffic to the website that the user will most likely know and trust, which it does by manipulating DNS records. The goal is to steal as much data as possible from the victim.
- Wifi Eavesdropping: Attackers allow victims to connect to the nearby wireless network. Kurbthinks it is connected to a secure network, but it is a malicious network designed for malicious purposes. It can monitor the user's online activity, scrape credit card information, login credentials.

2.10.2.How a Man-in-the-Middle (MITM) Attack Works

1. The victim sends a message to the other factor in the safe haven's safe.
2. The attacker intercepts the message without the knowledge of the other factor.
3. If the attacker modifies the content of the message, the attacker unknowingly eliminates the message on both sides.

MITM attacks can be obtained from unusual disconnections, strange URLs, or unsecured public wireless networks.

2.10.3.How to Prevent Man-in-the-Middle Attacks?

- Use end-to-end encryption.
- Connect to secure websites.
- Encrypt DNS traffic.
- Install patches, use anti-virus and keep track of updates.
- Remember the zero trust philosophy.
- Use strong passwords.
- Use a virtual network (VPN).