10 Types of Cyber Attacks You Should Be Aware in 2022

1. Malware Attack

This is one of the most common types of cyberattacks. “Malware” refers to malicious software viruses including worms, spyware, ransomware, adware, and trojans.

The trojan virus disguises itself as legitimate software. Ransomware blocks access to the network's key components, whereas Spyware is software that steals all your confidential data without your knowledge. Adware is software that displays advertising content such as banners on a user's screen.

Malware breaches a network through a vulnerability. When the user clicks a dangerous link, it downloads an email attachment or when an infected pen drive is used.

2. Phishing Attack

Phishing attacks are one of the most prominent widespread types of cyberattacks. It is a type of social engineering attack wherein an attacker impersonates to be a trusted contact and sends the victim fake mails.

Unaware of this, the victim opens the mail and clicks on the malicious link or opens the mail's attachment. By doing so, attackers gain access to confidential information and account credentials. They can also install malware through a phishing attack

3. Password Attack

It is a form of attack wherein a hacker cracks your password with various programs and password cracking tools like Aircrack, Cain, Abel, John the Ripper, Hashcat, etc. There are different types of password attacks like brute force attacks, dictionary attacks, and keylogger attacks.

4. Man-in-the-Middle Attack

A Man-in-the-Middle Attack (MITM) is also known as an eavesdropping attack. In this attack, an attacker comes in between a two-party communication, i.e., the attacker hijacks the session between a client and host. By doing so, hackers steal and manipulate data.

As seen below, the client-server communication has been cut off, and instead, the communication line goes through the hacker.

5. SQL Injection Attack

A Structured Query Language (SQL) injection attack occurs on a database-driven website when the hacker manipulates a standard SQL query. It is carried by injecting a malicious code into a vulnerable website search box, thereby making the server reveal crucial information.

This results in the attacker being able to view, edit, and delete tables in the databases. Attackers can also get administrative rights through this.

6. Denial-of-Service Attack

A Denial-of-Service Attack is a significant threat to companies. Here, attackers target systems, servers, or networks and flood them with traffic to exhaust their resources and bandwidth.

When this happens, catering to the incoming requests becomes overwhelming for the servers, resulting in the website it hosts either shut down or slow down. This leaves the legitimate service requests unattended.

It is also known as a DDoS (Distributed Denial-of-Service) attack when attackers use multiple compromised systems to launch this attack.

7. Insider Threat

As the name suggests, an insider threat does not involve a third party but an insider. In such a case; it could be an individual from within the organization who knows everything about the organization. Insider threats have the potential to cause tremendous damages.

Insider threats are rampant in small businesses, as the staff there hold access to multiple accounts with data. Reasons for this form of an attack are many, it can be greed, malice, or even carelessness. Insider threats are hard to predict and hence tricky.

8. Cryptojacking

The term Cryptojacking is closely related to cryptocurrency. Cryptojacking takes place when attackers access someone else’s computer for mining cryptocurrency.

The access is gained by infecting a website or manipulating the victim to click on a malicious link. They also use online ads with JavaScript code for this. Victims are unaware of this as the Crypto mining code works in the background; a delay in the execution is the only sign they might witness.

9. Zero-Day Exploit

A Zero-Day Exploit happens after the announcement of a network vulnerability; there is no solution for the vulnerability in most cases. Hence the vendor notifies the vulnerability so that the users are aware; however, this news also reaches the attackers.

Depending on the vulnerability, the vendor or the developer could take any amount of time to fix the issue. Meanwhile, the attackers target the disclosed vulnerability. They make sure to exploit the vulnerability even before a patch or solution is implemented for it.

10. Watering Hole Attack

The victim here is a particular group of an organization, region, etc. In such an attack, the attacker targets websites which are frequently used by the targeted group. Websites are identified either by closely monitoring the group or by guessing.

After this, the attackers infect these websites with malware, which infects the victims' systems. The malware in such an attack targets the user's personal information. Here, it is also possible for the hacker to take remote access to the infected computer.