Types of Cyber Attacks

A cyber attack refers to an action designed to target a computer or any element of a computerized information system to change, destroy, or steal data, as well as exploit or harm a network. Cyber attacks have been on the rise, in sync with the digitization of business that has become more and more popular in recent years.

1. DoS and DDoS Attacks

A DoS attack is designed to overwhelm the resources of a system to the point where it is unable to reply to legitimate service requests. A distributed denial-of-service (DDoS) attack is similar in that it also seeks to drain the resources of a system. A DDoS attack is initiated by a vast array of malware-infected host machines controlled by the attacker. These are referred to as “denial of service” attacks because the victim site is unable to provide service to those who want to access it.

2. Phishing Attacks

A attack occurs when a malicious actor sends emails that seem to be coming from trusted, legitimate sources in an attempt to grab sensitive information from the target. Phishing attacks combine engineeringand technology and are so-called because the attacker is, in effect, “fishing” for access to a forbidden area by using the “bait” of a seemingly trustworthy sender.
To execute the attack, the bad actor may send a link that brings you to a website that then fools you into downloading malware such as viruses, or giving the attacker your private information. In many cases, the target may not realize they have been compromised, which allows the attacker to go after others in the same organization without anyone suspecting malicious activity.

3. Whale-phishing Attacks

A whale-phishing attack is so-named because it goes after the “big fish” or whales of an organization, which typically include those in the C-suite or others in charge of the organization. These individuals are likely to possess information that can be valuable to attackers, such as proprietary information about the business or its operations.
If a targeted “whale” downloads ransomware, they are more likely to pay the ransom to prevent news of the successful attack from getting out and damaging their reputation or that of the organization. Whale-phishing attacks can be prevented by taking the same kinds of precautions to avoid phishing attacks, such as carefully examining emails and the attachments and links that come with them, keeping an eye out for suspicious destinations or parameters.

4. Ransomware

With ransomware, the victim’s system is held hostage until they agree to pay a ransom to the attacker. After the payment has been sent, the attacker then provides instructions regarding how the target can regain control of their computer. The name "ransomware” is appropriate because the malware demands a ransom from the victim. In a ransomware attack, the target downloads ransomware, either from a website or from within an email attachment. The malware is written to exploit vulnerabilities that have not been addressed by either the system's manufacturer or the IT team. The ransomware then encrypts the target's workstation. At times, ransomware can be used to attack multiple parties by denying access to either several computers or a central server essential to business operations.

5. SQL Injection Attack

SQL Injection is a common method of taking advantage of websites that depend on databases to serve their users. Clients are computers that get information from servers, and an SQL attack uses an SQL query sent from the client to a database on the server. The command is inserted, or "injected", into a data plane in place of something else that normally goes there, such as a password or login. The server that holds the database then runs the command and the system is penetrated. If an SQL injection succeeds, several things can happen, including the release of sensitive data or the modification or deletion of important data. Also, an attacker can execute administrator operations like a shutdown command, which can interrupt the function of the database.

6. DNS Spoofing

With Domain Name System (DNS) spoofing, a hacker alters DNS records to send traffic to a fake or "spoofed" website. Once on the fraudulent site, the victim may enter sensitive information that can be used or sold by the hacker. The hacker may also construct a poor-quality site with derogatory or inflammatory content to make a competitor company look bad. In a DNS spoofing attack, the attacker takes advantage of the fact that the user thinks the site they are visiting is legitimate. This gives the attacker the ability to commit crimes in the name of an innocent company, at least from the perspective of the visitor.

7. Brute force attack

A brute-force attack gets its name from the "brutish" or simple methodology employed by the attack. The attacker simply tries to guess the login credentials of someone with access to the target system. Once they get it right, they are in. While this may sound time-consuming and difficult, attackers often use bots to crack the credentials. The attacker provides the bot with a list of credentials that they think may give them access to the secure area. The bot then tries each one while the attacker sits back and waits. Once the correct credentials have been entered, the criminal gains access. To prevent brute-force attacks, have lock-out policies in place as part of your authorization security architecture. After a certain number of attempts, the user attempting to enter the credentials gets locked out. This typically involves "freezing" the account so even if someone else tries from a different device with a different IP address, they cannot bypass the lockout.

8. MITM Attacks

Man-in-the-middle (MITM) types of cyber attacks refer to breaches in cybersecurity that make it possible for an attacker to eavesdrop on the data sent back and forth between two people, networks, or computers. It is called a “man in the middle” attack because the attacker positions themselves in the “middle” or between the two parties trying to communicate. In effect, the attacker is spying on the interaction between the two parties. In a MITM attack, the two parties involved feel like they are communicating as they normally do. What they do not know is that the person actually sending the message illicitly modifies or accesses the message before it reaches its destination. Some ways to protect yourself and your organization from MITM attacks is by using strong encryption on access points or to use a virtual private network (VPN).