Common Types of Cyber Attacks

Cyber attacks are increasingly common, and some of the more advanced attacks can be launched without human intervention with the advent of network-based ransomware worms.

What is a Cyber Attack?

Definition of Cyber Attack: A cyber attack is when there is a deliberate and malicious attempt to breach the information system of an individual or organization.

While there is usually an economic goal, some recent attacks show the destruction of data as a goal. Malicious actors often look for ransom or other kinds of economic gain, but attacks can be perpetrated with an array of motives, including political activism purposes.

Top 10 common types of cyber security attacks

- Malware
- Phishing
- Man-in-the-Middle (MitM) Attacks
- Denial-of-Service (DOS) Attack
- SQL Injections
- Zero-day Exploit
- Password Attack
- Cross-site Scripting
- Rootkits
- Internet of Things (IoT) Attacks

Malware

Malware or Malicious software is the term that encompasses various types of attacks including spyware, viruses, and worms. Malware uses a vulnerability to breach a network when a user clicks a “planted” dangerous link or email attachment, which is used to install malicious software inside the system.

Malware and malicious files inside a computer system can:

- Deny access to the critical components of the network
- Obtain information by retrieving data from the hard drive
- Disrupt the system or even render it inoperable

Malware is so common that there is a large variety of modus operandi. The most common types being:

- **Ransomware**: This type of malware encrypts a user's files and demands payment in exchange for the decryption key. It's a significant threat to IT systems as it can cause data loss, downtime, and financial losses.
- **Fileless Malware:** Unlike traditional malware, fileless malware operates in a system's memory without leaving any files behind. As it's difficult to detect, it can cause damage to IT systems, steal sensitive data, and take control of the infected device.

- **Spyware:** This type of malware secretly collects information about a user without their knowledge or consent. It's a threat to IT systems as it can steal sensitive information such as login credentials, banking information, and personal data.
- **Adware:** Adware is malware that displays unwanted advertisements and redirects users to potentially harmful websites. It can slow down IT systems and expose users to further malware infections.
- **Trojans:** A trojan appears as legitimate software but has malicious intent, often used to steal data or gain access to a system. It's a significant threat to IT systems as it can be challenging to detect and can cause serious damage.
- **Worms:** A worm is self-replicating malware that spreads across networks and can cause widespread damage. It's a threat to IT systems as it can consume network bandwidth and cause significant disruption.

- **Rootkits:** Rootkits conceal malware by altering system behavior and evading detection. They can take control of IT systems, steal sensitive data, and cause damage without being detected.
- **Mobile Malware:** Mobile malware targets mobile devices and can access sensitive data, control the device, or generate revenue through fraudulent activities. It's a growing threat to IT systems as mobile usage continues to rise.
- **Exploits:** Exploits take advantage of vulnerabilities in software or systems to gain access or cause harm. They are a significant threat to IT systems as they can be used to install further malware, steal data, or take control of devices.
- **Scareware:** Scareware is misleading software that tricks users into believing their system is infected, prompting them to purchase fake antivirus software. It can cause financial losses and expose users to further malware infections.
- **Keylogger:** A keylogger is malware that records keystrokes on a device, allowing an attacker to steal sensitive information such as login credentials, credit card information, and personal data.
- **Botnet:** A botnet is a network of infected devices that can be controlled by an attacker to perform malicious activities. It can be used to launch large-scale attacks, steal sensitive information, and generate revenue through fraudulent activities.

Phishing

Phishing attacks are extremely common and involve sending mass amounts of fraudulent emails to unsuspecting users, disguised as coming from a

reliable source. The fraudulent emails often have the appearance of being legitimate, but link the recipient to a malicious file or script designed to grant attackers access to your device to control it or gather recon, install malicious scripts/files, or to extract data such as user information, financial info, and more.

Phishing attacks can also take place via social networks and other online communities, via direct messages from other users with a hidden intent. Phishers often leverage social engineering and other public information sources to collect info about your work, interests, and activities—giving attackers an edge in convincing you they're not who they say.

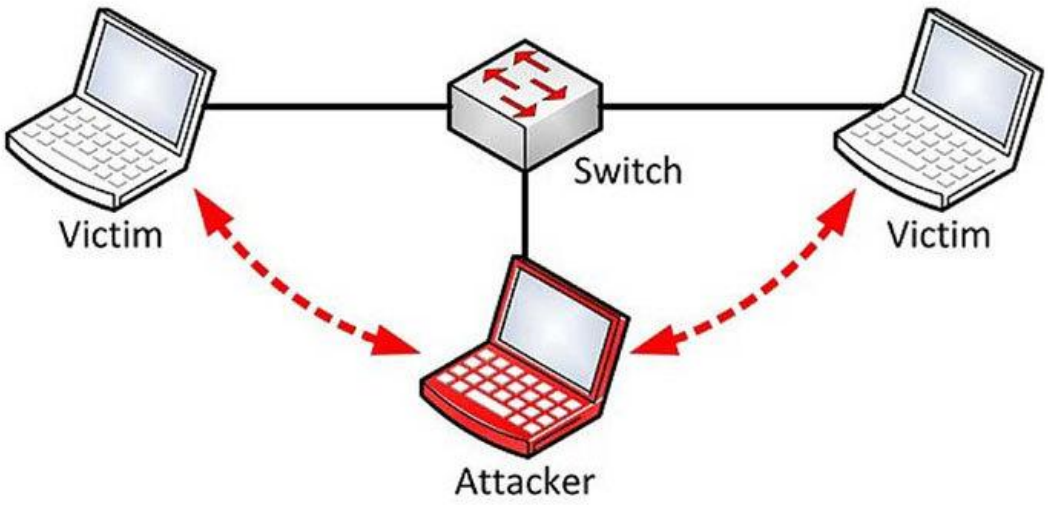
There are several different types of phishing attacks, including:

- **Spear Phishing**—targeted attacks directed at specific companies and/or individuals.
- **Whaling**—attacks targeting senior executives and stakeholders within an organization.
- **Pharming**—leverages DNS cache poisoning to capture user credentials through a fake login landing page.

Phishing attacks can also take place via phone call (voice phishing) and via text message (SMS phishing). This post highlights additional details about phishing attacks—how to spot them and how to prevent them.

Man-in-the-Middle (MitM) Attacks

Occurs when an attacker intercepts a two-party transaction, inserting themselves in the middle. From there, cyber attackers can steal and manipulate data by interrupting traffic.



This type of attack usually exploits security vulnerabilities in a network, such as an unsecured public WiFi, to insert themselves between a visitor's device and the network. The problem with this kind of attack is that it is very difficult to detect, as the victim

thinks the information is going to a legitimate destination. Phishing or malware attacks are often leveraged to carry out a MitM attack.

Denial-of-Service (DOS) Attack

DoS attacks work by flooding systems, servers, and/or networks with traffic to overload resources and bandwidth. The result is rendering the system unable to process and fulfill legitimate requests. In addition to denial-of-service (DoS) attacks, there are also distributed denial-of-service (DDoS) attacks.

DoS attacks saturate a system's resources with the goal of impeding response to service requests. On the other hand, a DDoS attack is launched from several infected host machines with the goal of achieving service denial and taking a system offline, thus paving the way for another attack to enter the network/environment.

The most common types of DoS and DDoS attacks are the TCP SYN flood attack, teardrop attack, smurf attack, ping-of-death attack, and botnets.

SQL Injections

This occurs when an attacker inserts malicious code into a server using server query language (SQL) forcing the server to deliver protected information. This type of attack usually involves submitting malicious code into an unprotected website comment or search box. Secure coding practices such as using prepared statements with parameterized queries is an effective way to prevent SQL injections.

When a SQL command uses a parameter instead of inserting the values directly, it can allow the backend to run malicious queries. Moreover, the SQL interpreter uses the parameter only as data, without executing it as a code. Learn more about how secure coding practices can prevent SQL injection here.

Zero-day Exploit

A Zero-day Exploit refers to exploiting a network vulnerability when it is new and recently announced — before a patch is released and/or implemented. Zero-day attackers jump at the disclosed vulnerability in the small window of time where no

solution/preventative measures exist. Thus, preventing zero-day attacks requires constant monitoring, proactive detection, and agile threat management practices.

Password Attack

Passwords are the most widespread method of authenticating access to a secure information system, making them an attractive target for cyber attackers. By accessing a person's password, an attacker can gain entry to confidential or critical data and systems, including the ability to manipulate and control said data/systems.

Password attackers use a myriad of methods to identify an individual password, including using social engineering, gaining access to a password database, testing the network connection to obtain unencrypted passwords, or simply by guessing.

The last method mentioned is executed in a systematic manner known as a "brute-force attack." A brute-force attack employs a program to try all the possible variants and combinations of information to guess the password.

Another common method is the dictionary attack, when the attacker uses a list of common passwords to attempt to gain access to a user's computer and network.

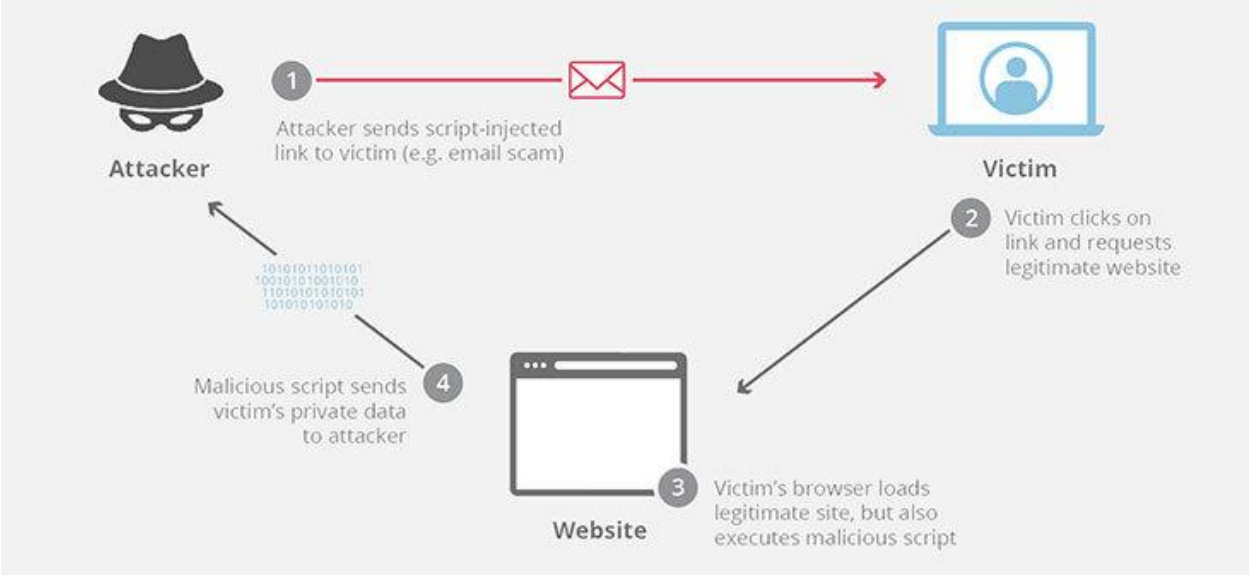
Account lockout best practices and two-factor authentication are very useful at preventing a password attack. Account lockout features can freeze the account out after a number of invalid password attempts and two-factor authentication adds an additional

layer of security, requiring the user logging in to enter a secondary code only available on their 2FA device(s).

Cross-site Scripting

A cross-site scripting attack sends malicious scripts into content from reliable websites. The malicious code joins the dynamic content that is sent to the victim's browser.

Usually, this malicious code consists of Javascript code executed by the victim's browser, but can include Flash, HTML, and XSS.



Additional information about cross-site scripting attacks can be found here.

Rootkits

Rootkits are installed inside legitimate software, where they can gain remote control and administration-level access over a system. The attacker then uses the rootkit to steal passwords, keys, credentials, and retrieve critical data.

Since rootkits hide in legitimate software, once you allow the program to make changes in your OS, the rootkit installs itself in the system (host, computer, server, etc.) and remains dormant until the attacker activates it or it's triggered through a persistence mechanism. Rootkits are commonly spread through email attachments and downloads from insecure websites.

Internet of Things (IoT) Attacks

While internet connectivity across almost every imaginable device creates convenience and ease for individuals, it also presents a growing—almost unlimited—number of access points for attackers to exploit and wreak havoc. The interconnectedness of things makes it possible for attackers to breach an entry point and use it as a gate to exploit other devices in the network.

IoT attacks are becoming more popular due to the rapid growth of IoT devices and (in general) low priority given to embedded security in these devices and their operating systems. In one IoT attack case, a Vegas casino was attacked and the hacker gained entry via an internet-connected thermometer inside one of the casino's fishtanks.

Best practices to help prevent an IoT attack include updating the OS and keeping a strong password for every IoT device on your network, and changing passwords often.

How to mitigate against cyber attacks

The complexity and variety of cyberattacks are ever-increasing, with a different type of attack for every nefarious purpose. While cybersecurity prevention measures differ for each type of attack, good security practices and basic IT hygiene are generally good at mitigating these attacks.

In addition to implementing good cybersecurity practices, your organization should exercise secure coding practices, keep systems and security software up to date, leverage firewalls and threat management tools and solutions, install antivirus software across systems, control access and user privileges, backup systems often, and

proactively watch for breached systems with a managed detection and response service.