**Cybersecurity Threats**

Cybersecurity threats are acts performed by individuals with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems. Common categories of cyber threats include malware, social engineering, man in the middle (MitM) attacks, denial of service (DoS) and injection attacks.

Cyber threats can originate from a variety of sources, from hostile nation states and terrorist groups, to individual hackers, to trusted individuals like employees or contractors, who abuse their privileges to perform malicious acts.

**Common Sources of Cyber Threats**

Here are several common sources of cyber threats against organizations:

* **Nation states**—hostile countries can launch cyber-attacks against local companies and institutions, aiming to interfere with communications, cause disorder, and inflict damage.
* **Terrorist organizations**—terrorists conduct cyber-attacks aimed at destroying or abusing critical infrastructure, threaten national security, disrupt economies, and cause bodily harm to citizens.
* **Criminal groups**—organized groups of hackers aim to break into computing systems for economic benefit. These groups use phishing, spam, spyware and malware for extortion, theft of private information, and online scams.
* **Hackers**—individual hackers target organizations using a variety of attack techniques. They are usually motivated by personal gain, revenge, financial gain, or political activity. Hackers often develop new threats, to advance their criminal ability and improve their personal standing in the hacker community.
* **Malicious insiders**—an employee who has legitimate access to company assets, and abuses their privileges to steal information or damage computing systems for economic or personal gain. Insiders may be employees, contractors, suppliers, or partners of the target organization. They can also be outsiders who have compromised a privileged account and are impersonating its owner.

**Types of Cybersecurity Threats**

**Malware Attacks**

Malware is an abbreviation of “malicious software”, which includes viruses, worms, trojans, spyware, and ransomware, and is the most common type of cyberattack. Malware infiltrates a system, usually via a link on an untrusted website or email or an unwanted software download. It deploys on the target system, collects sensitive data, manipulates and blocks access to network components, and may destroy data or shut down the system altogether.

Here are some of the main types of malware attacks:

* **Viruses—**a piece of code injects itself into an application. When the application runs, the malicious code executes.
* **Worms—**malware that exploits software vulnerabilities and backdoors to gain access to an operating system. Once installed in the network, the worm can carry out attacks such as distributed denial of service (DDoS).
* **Trojans—**malicious code or software that poses as an innocent program, hiding in apps, games or email attachments. An unsuspecting user downloads the trojan, allowing it to gain control of their device.
* **Ransomware—**a user or organization is denied access to their own systems or data via encryption. The attacker typically demands a ransom be paid in exchange for a decryption key to restore access, but there is no guarantee that paying the ransom will actually restore full access or functionality.
* **Cryptojacking**—attackers deploy software on a victim’s device, and begin using their computing resources to generate cryptocurrency, without their knowledge. Affected systems can become slow and cryptojacking kits can affect system stability.
* **Spyware**—a malicious actor gains access to an unsuspecting user’s data, including sensitive information such as passwords and payment details. Spyware can affect desktop browsers, mobile phones and desktop applications.
* **Adware—**a user’s browsing activity is tracked to determine behavior patterns and interests, allowing advertisers to send the user targeted advertising. Adware is related to spyware but does not involve installing software on the user’s device and is not necessarily used for malicious purposes, but it can be used without the user’s consent and compromise their privacy.
* **Fileless malware**—no software is installed on the operating system. Native files like WMI and PowerShell are edited to enable malicious functions. This stealthy form of attack is difficult to detect (antivirus can’t identify it), because the compromised files are recognized as legitimate.
* **Rootkits—**software is injected into applications, firmware, operating system kernels or hypervisors, providing remote administrative access to a computer. The attacker can start the operating system within a compromised environment, gain complete control of the computer and deliver additional malware.

**Social Engineering Attacks**

Social engineering involves tricking users into providing an entry point for malware. The victim provides sensitive information or unwittingly installs malware on their device, because the attacker poses as a legitimate actor.

Here are some of the main types of social engineering attacks:

* **Baiting**—the attacker lures a user into a social engineering trap, usually with a promise of something attractive like a free gift card. The victim provides sensitive information such as credentials to the attacker.
* **Pretexting**—similar to baiting, the attacker pressures the target into giving up information under false pretenses. This typically involves impersonating someone with authority, for example an IRS or police officer, whose position will compel the victim to comply.
* **Phishing—**the attacker sends emails pretending to come from a trusted source. Phishing often involves sending fraudulent emails to as many users as possible, but can also be more targeted. For example, “spear phishing” personalizes the email to target a specific user, while “whaling” takes this a step further by targeting high-value individuals such as CEOs.
* **Vishing**(voice phishing)—the imposter uses the phone to trick the target into disclosing sensitive data or grant access to the target system. Vishing typically targets older individuals but can be employed against anyone.
* **Smishing**(SMS phishing)—the attacker uses text messages as the means of deceiving the victim.
* **Piggybacking**—an authorized user provides physical access to another individual who “piggybacks” off the user’s credentials. For example, an employee may grant access to someone posing as a new employee who misplaced their credential card.
* **Tailgating—**an unauthorized individual follows an authorized user into a location, for example by quickly slipping in through a protected door after the authorized user has opened it. This technique is similar to piggybacking except that the person being tailgated is unaware that they are being used by another individual.

**Supply Chain Attacks**

Supply chain attacks are a new type of threat to software developers and vendors. Its purpose is to infect legitimate applications and distribute malware via source code, build processes or software update mechanisms.

Attackers are looking for non-secure network protocols, server infrastructure, and coding techniques, and use them to compromise build and update process, modify source code and hide malicious content.

Supply chain attacks are especially severe because the applications being compromised by attackers are signed and certified by trusted vendors. In a software supply chain attack, the software vendor is not aware that its applications or updates are infected with malware. Malicious code runs with the same trust and privileges as the compromised application.

Types of supply chain attacks include:

* **Compromise of build tools** or development pipelines
* **Compromise of code signing procedures** or developer accounts
* **Malicious code sent as automated updates** to hardware or firmware components
* **Malicious code pre-installed**on physical devices

**Man-in-the-Middle Attack**

A Man-in-the-Middle (MitM) attack involves intercepting the communication between two endpoints, such as a user and an application. The attacker can eavesdrop on the communication, steal sensitive data, and impersonate each party participating in the communication.

Examples of MitM attacks include:

* **Wi-Fi eavesdropping—**an attacker sets up a Wi-Fi connection, posing as a legitimate actor, such as a business, that users may connect to. The fraudulent Wi-Fi allows the attacker to monitor the activity of connected users and intercept data such as payment card details and login credentials.
* **Email hijacking**—an attacker spoofs the email address of a legitimate organization, such as a bank, and uses it to trick users into giving up sensitive information or transferring money to the attacker. The user follows instructions they think come from the bank but are actually from the attacker.
* **DNS spoofing**—a Domain Name Server (DNS) is spoofed, directing a user to a malicious website posing as a legitimate site. The attacker may divert traffic from the legitimate site or steal the user’s credentials.
* **IP spoofing**—an internet protocol (IP) address connects users to a specific website. An attacker can spoof an IP address to pose as a website and deceive users into thinking they are interacting with that website.
* **HTTPS spoofing**—HTTPS is generally considered the more secure version of HTTP, but can also be used to trick the browser into thinking that a malicious website is safe. The attacker uses “HTTPS” in the URL to conceal the malicious nature of the website.

**Denial-of-Service Attack**

A Denial-of-Service (DoS) attack overloads the target system with a large volume of traffic, hindering the ability of the system to function normally. An attack involving multiple devices is known as a distributed denial-of-service (DDoS) attack.

DoS attack techniques include:

* **HTTP flood DDoS**—the attacker uses HTTP requests that appear legitimate to overwhelm an application or web server. This technique does not require high bandwidth or malformed packets, and typically tries to force a target system to allocate as many resources as possible for each request.
* **SYN flood DDoS**—initiating a Transmission Control Protocol (TCP) connection sequence involves sending a SYN request that the host must respond to with a SYN-ACK that acknowledges the request, and then the requester must respond with an ACK. Attackers can exploit this sequence, tying up server resources, by sending SYN requests but not responding to the SYN-ACKs from the host.
* **UDP flood DDoS**—a remote host is flooded with User Datagram Protocol (UDP) packets sent to random ports. This technique forces the host to search for applications on the affected ports and respond with “Destination Unreachable” packets, which uses up the host resources.
* **ICMP flood**—a barrage of ICMP Echo Request packets overwhelms the target, consuming both inbound and outgoing bandwidth. The servers may try to respond to each request with an ICMP Echo Reply packet, but cannot keep up with the rate of requests, so the system slows down.
* **NTP amplification**—Network Time Protocol (NTP) servers are accessible to the public and can be exploited by an attacker to send large volumes of UDP traffic to a targeted server. This is considered an amplification attack due to the query-to-response ratio of 1:20 to 1:200, which allows an attacker to exploit open NTP servers to execute high-volume, high-bandwidth DDoS attacks.

**Injection Attacks**

Injection attacks exploit a variety of vulnerabilities to directly insert malicious input into the code of a web application. Successful attacks may expose sensitive information, execute a DoS attack or compromise the entire system.

Here are some of the main vectors for injection attacks:

* **SQL injection**—an attacker enters an SQL query into an end user input channel, such as a web form or comment field. A vulnerable application will send the attacker’s data to the database, and will execute any SQL commands that have been injected into the query. Most web applications use databases based on Structured Query Language (SQL), making them vulnerable to SQL injection. A new variant on this attack is NoSQL attacks, targeted against databases that do not use a relational data structure.
* **Code injection**—an attacker can inject code into an application if it is vulnerable. The web server executes the malicious code as if it were part of the application.
* **OS command injection**—an attacker can exploit a command injection vulnerability to input commands for the operating system to execute. This allows the attack to exfiltrate OS data or take over the system.
* **LDAP injection**—an attacker inputs characters to alter Lightweight Directory Access Protocol (LDAP) queries. A system is vulnerable if it uses unsanitized LDAP queries. These attacks are very severe because LDAP servers may store user accounts and credentials for an entire organization.
* **XML eXternal Entities (XXE) Injection**—an attack is carried out using specially-constructed XML documents. This differs from other attack vectors because it exploits inherent vulnerabilities in legacy XML parsers rather than unvalidated user inputs. XML documents can be used to traverse paths, execute code remotely and execute server-side request forgery (SSRF).
* **Cross-Site Scripting (XSS)**—an attacker inputs a string of text containing malicious JavaScript. The target’s browser executes the code, enabling the attacker to redirect users to a malicious website or steal session cookies to hijack a user’s session. An application is vulnerable to XSS if it doesn’t sanitize user inputs to remove JavaScript code.

**Cybersecurity Solutions**

Cybersecurity solutions are tools organizations use to help defend against cybersecurity threats, as well as accidental damage, physical disasters, and other threats. Here are the main types of security solutions:

* **Application security**—used to test software application vulnerabilities during development and testing, and protect applications running in production, from threats like network attacks, exploits of software vulnerabilities, and web application attacks.
* **Network security—**monitors network traffic, identifies potentially malicious traffic, and enables organizations to block, filter or mitigate threats.
* **Cloud Security—**implements security controls in public, private and hybrid cloud environments, detecting and fixing false security configurations and vulnerabilities.
* **Endpoint security—**deployed on endpoint devices such as servers and employee workstations, which can prevent threats like malware, unauthorized access, and exploitation of operating system and browser vulnerabilities.
* **Internet of Things (IoT) security—**connected devices are often used to store sensitive data, but are usually not protected by design. IoT security solutions help gain visibility and improve security for IoT devices.
* **Threat intelligence**—combines multiple feeds containing data about attack signatures and threat actors, providing additional context for security events. Threat intelligence data can help security teams detect attacks, understand them, and design the most appropriate response.