Advanced Persistent Threat (APT)

An advanced persistent threat (APT) is a prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period of time. APT attacks are initiated to steal data rather than cause damage to the target organization's network.

Ransomware

Ransomware is a malware designed to make a target’s data unusable or to prevent access to systems until a ransom – typically in hard-to-trace digital currency - is paid.

Malware

Malware is a term used to describe malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software. Once inside the system, malware can do the following:

* Blocks access to key components of the network (ransomware)
* Installs malware or additional harmful software
* Covertly obtains information by transmitting data from the hard drive (spyware)
* Disrupts certain components and renders the system inoperable

Phishing

Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim’s machine. Phishing is an increasingly common cyberthreat.

Man-in-the-middle attack

Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.

Two common points of entry for MitM attacks:

1. On unsecure public Wi-Fi, attackers can insert themselves between a visitor’s device and the network. Without knowing, the visitor passes all information through the attacker.

2. Once malware has breached a device, an attacker can install software to process all of the victim’s information.

Denial-of-service attack

A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. Attackers can also use multiple compromised devices to launch this attack. This is known as a [distributed-denial-of-service (DDoS) attack](https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html).

SQL injection

A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.

Zero-day exploit

A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time. [Zero-day vulnerability threat detection](https://www.talosintelligence.com/vulnerability_reports) requires constant awareness.

DNS Tunneling

DNS tunneling utilizes the DNS protocol to communicate non-DNS traffic over port 53. It sends HTTP and other protocol traffic over DNS. There are various, legitimate reasons to utilize DNS tunneling. However, there are also malicious reasons to use DNS Tunneling VPN services. They can be used to disguise outbound traffic as DNS, concealing data that is typically shared through an internet connection. For malicious use, DNS requests are manipulated to exfiltrate data from a compromised system to the attacker’s infrastructure. It can also be used for command-and-control callbacks from the attacker’s infrastructure to a compromised system.

Social engineering Attacks

**Indicator**

Request from a stranger to perform a suspicious activity

Sense of urgency and pressure to complete the request immediately

Anger or hesitancy if you ask for proof of identity

**Defenses**

Challenge the requester’s identity

Verify the suspicious request with your supervisor

Slow down or pause the interaction