# ADVANCED PERSISTENT THREAT

**ABOUT APT**

* A targeted cyberattack that can go undetected for months or years.
* Typically carried out by nation-states or state-sponsored groups.
* Aims to steal sensitive data or disrupt operations.
* Can be difficult to detect and respond to.

Here are some additional details about APT attacks:

* They are often targeted at specific organizations or individuals.
* The attackers will have done extensive research on their target, in order to understand their security weaknesses and how to exploit them.
* APT attacks use sophisticated techniques, such as spear phishing, zero-day exploits, and malware. These techniques are designed to bypass traditional security measures.
* APT attacks are difficult to detect, because they are so well-planned and executed. The attackers will often use a variety of techniques to cover their tracks, making it difficult for security analysts to identify the attack.

## Characteristics of an APT Attack

* **Targeted**: APT attacks are typically targeted at specific organizations or individuals. The attackers will often conduct extensive research on their target in order to identify vulnerabilities and develop a tailored attack plan.
* **Sophisticated:** APT attacks often use sophisticated techniques, such as zero-day exploits, social engineering, and spear phishing. These techniques can be very difficult to defend against, even for well-protected organizations.
* **Stealth:** APT attackers are very good at hiding their tracks. They often use custom malware that is designed to evade detection by traditional security tools.
* **Longevity:** APT attacks can last for months or even years. The attackers will often establish a presence in the victim's network and then slowly gather information over time.

**APT EMERGING TRENDS**

* **The use of new attack vectors**. APT attackers are constantly looking for new ways to infiltrate networks. This includes using new malware, exploiting zero-day vulnerabilities, and targeting new industries and sectors.
* **The use of social engineering techniques**. APT attackers are very good at using social engineering techniques to trick victims into clicking on malicious links or opening infected attachments. This is often the first step in an APT attack.
* **The use of targeted spear phishing attacks**. APT attackers often target specific individuals or organizations with spear phishing attacks. These attacks are more likely to be successful because they are tailored to the specific victim.
* **The use of supply chain attacks**. APT attackers are increasingly targeting the supply chain of organizations. This means that they are attacking the companies that provide software, hardware, or services to their targets.
* **The use of ransomware**. Ransomware is becoming increasingly popular among APT attackers. This is because it can be a very effective way to extort money from victims.

**APT Detection**

 New tactics and techniques are created to stay a step ahead of detection. While it’s difficult to detect a persistent threat and have a quick APT solution, it’s not impossible. The next step is to understand how attackers operate to identify the best ways to detect their activities. Two primary methods of detecting persistent threats are tracking and analysis.

### 1. Email filtering

During email filtering, the software automatically moves unwanted emails to a separate folder after analyzing them for red flags that signal phishing. You are more likely to lose your personal sensitive information such as banking or identity number when you click on a phishing email. The sole purpose of phishing emails is to steal your personal information.

### 2. Endpoint protection

Data and workflows associated with individual devices on your network are protected through endpoint security. Endpoint protection platforms examine files as they enter the network. With endpoint security, you'll not only be protected from malicious software, you'll also be protected against evolving zero-day threats.

### 3. Access control

Providing access to and using company information and resources is a fundamental component of data security. By authenticating and authorizing users, access control policies ensure they have access to company data in accordance with their claims.

### 4. Monitoring of traffic, user and entity behavior

Monitoring network events generated each day by users, users, and entities is the process of gathering insight into their behavior. By collecting and analyzing this data, you can identify compromised credentials, lateral movement, and other malicious activity.