ADVANCED PRESISTENT THREAT

(APT)

INDEX

What is an Advanced Persistent Threat?

- An advanced persistent threat is an attack in which an unauthorized user gains access to a system or network and remains there for an extended period of time without being detected. Advanced persistent threats are particularly dangerous for enterprises, as hackers have ongoing access to sensitive company data. Advanced persistent threats generally do not cause damage to company networks or local machines. Instead, the goal of advanced persistent threats is most often data theft.
- Advanced persistent threats typically have several phases, including hacking the network, avoiding detection, constructing a plan of attack and mapping company data to determine where the desired data is most accessible, gathering sensitive company data, and exfiltrating that data.
- Advanced persistent threats have caused several large, costly data breaches and are known for their ability to fly under the radar, remaining undetectable by traditional security measures. What's more, advanced persistent threats are becoming increasingly common as cyber criminals look to more sophisticated measures to achieve their goals.

What are the 3 Stages of an APT Attack?

- **Stage 1: Infiltration**

  In the first phase, **advanced persistent threats often gain access through social engineering techniques**. One indication of an APT is a phishing email that selectively targets high-level individuals like senior executives or technology leaders, often using information obtained from other team members that have already been compromised. Email attacks that target specific individuals are called "spear-phishing."

  The email may seem to come from a team member and include references to an ongoing project. If several executives report being duped by a spear-phishing attack, start looking for other signs of an APT.

- **Stage 2: Escalation and Lateral Movement**

  Once initial access has been gained, attackers insert malware into an organization's network to move to the second phase, expansion. They **move laterally to map the network and gather credentials** such as account names and passwords in order to access critical business information.

  They may also establish a "backdoor" — a scheme that allows them to sneak into the network later to conduct stealth operations. Additional entry points are often established to ensure that the attack can continue if a compromised point is discovered and closed.

- **Stage 3: Exfiltration**

  To prepare for the third phase, cybercriminals typically **store stolen information in a secure location** within the network until enough data has been collected. They **then extract, or "exfiltrate" it without detection**. They may use tactics like a denial-of-service (DoS) attack to distract the security team and tie up network personnel while the data is being exfiltrated. The network can remain compromised, waiting for the thieves to return at any time.

Advanced Persistent Threat Examples

- **CrowdStrike currently tracks well over 150 adversaries** around the world, including nation-states, eCriminals and hacktivists.

  Here are some notable examples of APTs detected by CrowdStrike:

- **GOBLIN PANDA** (APT27) was first observed in September 2013 when CrowdStrike discovered indicators of attack (IOAs) in the network of a technology company that operates in multiple sectors. This China-based adversary uses two Microsoft Word exploit documents with training-related themes to drop malicious files when opened.
- **FANCY BEAR** (APT28), a Russia-based attacker, uses phishing messages and spoofed websites that closely resemble legitimate ones in order to gain access to conventional computers and mobile devices.
- **Cozy Bear** (APT29) is an adversary of Russian-origin, assessed as likely to be acting on behalf of the Foreign Intelligence Service of the Russian Federation. This adversary has been identified leveraging large-volume spear phishing campaigns to deliver an extensive range of malware types as part of an effort to target political, scientific, and national security entities across a variety of sectors.
- **Ocean Buffalo** (APT32) is a Vietnam-based targeted intrusion adversary reportedly active since at least 2012. This adversary is known to employ a wide range of Tactics, Techniques, and Procedures (TTPs), to include the use of both custom and off-the-shelf tools as well as the distribution of malware via Strategic Web Compromise (SWC) operations and spear phishing emails containing malicious attachments.
- **HELIX KITTEN** (APT34) has been active since at least late 2015 and is likely Iran-based. It targets organizations in aerospace, energy, financial, government, hospitality and telecommunications and uses well researched and structured spear-phishing messages that are highly relevant to targeted personnel.
- **Wicked Panda** (APT41) has been one the most prolific and effective China-based adversaries from the mid-2010s into the 2020s. CrowdStrike Intelligence assesses Wicked Panda consists of a superset of groups involving several contractors working in the interests of the Chinese state while still carrying out criminal, for-profit activities, likely with some form of tacit approval from CCP officials.

How do you Protect against APT Attacks?

There are many cybersecurity and intelligence solutions available to assist organizations in better protecting against APT attacks. Here are some of the best tactics to employ:

- **Sensor Coverage.** Organizations must deploy capabilities that provide their defenders with full visibility across their environment to avoid blind spots that can become a safe haven for cyber threats.
- **Technical Intelligence.** Leverage technical intelligence, such as indicators of compromise (IOCs), and consume them into a security information and event manager (SIEM) for data enrichment purposes. This allows for added intelligence when conducting event correlation, potentially highlighting events on the network that may have otherwise gone undetected.
- **Service Provider.** Collaborating with a best-of-breed cybersecurity firm is a necessity. Should the unthinkable happen, organizations might require assistance responding to a sophisticated cyber threat?
- A **Web Application Firewall (WAF)** is a security device designed to protect organizations at the application level by filtering, monitoring and analyzing hypertext transfer protocol (HTTP) and hypertext transfer protocol secure (HTTPS) traffic between the web application and the internet.
- **Threat Intelligence.** Threat intelligence assists with threat actor profiling, campaign tracking and malware family tracking. These days, it is more important to understand the context of an attack rather than just knowing an attack, itself happened, and this is where threat intelligence plays a vital role.
- **Threat Hunting.** Many organizations will find the need for 24/7, managed, human-based threat hunting to accompany their cybersecurity technology already in place.

CHARACTERSTICS OF AN APT ATTACK

- TARGETED
- SOPHISTICATED
- STEALTH
- LONGEVITY
- ADVANCED TECHNIQUES
- PERSISTENCE
- COVERT OPERATIONS
- MULTI-STAGE ATTACKS
- NATION-STATE OR WELL -RESOURCED ACTORS
- SPECIFIC OBJECTIVES

- **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.

- Advanced Techniques: APT attackers employ advanced and sophisticated techniques to bypass traditional security defenses. They may utilize zero-day exploits, custom malware, or techniques that evade detection by security solutions.
- Persistence: APTs are designed to maintain long-term presence within the targeted network or system. Attackers employ stealthy methods to establish backdoors, create hidden user accounts, or install persistent malware that can evade detection.
- Targeted Approach: APTs are specifically tailored to target particular organizations, industries, or individuals. Attackers conduct extensive reconnaissance to gather information about the target's infrastructure, vulnerabilities, and potential points of entry.
- Covert Operations: APT attackers focus on remaining undetected for an extended period to accomplish their objectives. They often use advanced evasion techniques, encryption, and anti-forensic measures to hide their activities and avoid detection by security monitoring systems.
- Multi-Stage Attacks: APTs typically involve multiple stages and tactics. Attackers may use initial compromise techniques like spear-phishing, watering hole attacks, or supply chain attacks to gain a foothold. They then progress through various stages, including lateral movement, privilege escalation, data exfiltration, and persistence.
- Nation-State or Well-Resourced Actors: APTs are often associated with nation-state actors or well-funded organizations. These adversaries have significant resources, including skilled personnel, financial backing, and access to advanced tools and technologies.

ATP EMERGING TRENDS

- THE USE OF NEW ATTACK VECTORS.
- THE USE OF SOCIAL ENGINEERING TECHNIQUES.
- THE USE OF TARGETED SPARE PHISHING ATTACKS.
- THE USE OF SUPPLY CHAIN ATTACKS.
- THE USE OF RANSOMWARE.

- **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.

ATP 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.

- EMAIL FILTERING
- ENDPOINT PROTECTION
- ACCESS CONTROL
- MONITORING OF TRAFFIC, USER AND ENTITY BEHAVIOR

- **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.

CONCLUSION

- Advanced persistent threat attacks pose a serious risk to organizations and can result in the loss of critical information. To prevent these attacks, you must understand the hackers and what they are trying to do on your network. The best way to prevent an advanced persistent threat attack is to secure your systems and prevent unauthorized access. Many APT protection tools are available that can help you do this, and many are free.
- One of the best advanced persistent threat prevention is you need to protect your systems and prevent unauthorized access. These hackers often use legitimate tools and methods to achieve their goals and the best way to prevent them is to secure your systems and prevent unauthorized access.