What is an advanced persistent threat (APT)?

An advanced persistent threat (APT) is a prolonged and targeted cyber attack in which an intruder gains access to a network and remains undetected for an extended period.

APT attacks are initiated to steal highly sensitive data rather than cause damage to the target organization's network. The goal of most APT attacks is to achieve and maintain ongoing access to the targeted network rather than to get in and out as quickly as possible.

Unlike ransomware as a service and other cyber assaults, APTs are executed manually through meticulous planning. Because a great deal of effort and resources can go into carrying out APT attacks, threat actors typically select high-value targets, such as large organizations, to steal information over a long period. For this reason, APT attacks are typically orchestrated by well-funded nation-state cybercriminal groups rather than individual hackers.

Which techniques are used in an APT attack?

To gain access, APT groups often use a variety of advanced attack methods, including social engineering techniques. To maintain access to the targeted network without being discovered, threat actors continuously rewrite malicious code to avoid detection and other sophisticated evasion techniques. In fact, some APTs are so complex that they require full-time administrators to maintain the compromised systems and software in the targeted network.

Common techniques used during APT attacks include the following:

- **Spear phishing.** APT actors commonly use highly targeted spear phishing emails to fool people into divulging personal information or clicking on harmful links that can execute malicious code into their systems. These emails are skillfully written to appear authentic and tailored to the recipient.
- **Zero-day exploits.** APT actors often take advantage of zero-day vulnerabilities in software or hardware that have recently been discovered but not yet patched. By exploiting the vulnerabilities before they've been addressed, threat actors can easily gain unauthorized access to target systems.
- **Watering hole attacks.** APT actors use the watering hole attack to breach websites often accessed by their specific targets. By injecting malicious code into these websites, they can infect the systems of unsuspecting visitors.
- **Supply chain attacks.** Supply chain attacks target a specific organization's supply chain, compromising software or hardware before it reaches the intended receiver. This lets APT actors gain access to the victim's network.

- ***Credential theft.*** *APT actors use methods such as keylogging, password cracking and credential phishing to obtain login credentials. Once they have legitimate credentials, they can navigate the network laterally and gain access to sensitive information.*
- ***Command-and-control (C&C) servers.*** *Using C&C servers, APTs create communication routes between hacked systems and their network. This lets the attacker maintain control over the compromised network and exfiltrate data.*
- ***Evasion strategies.*** *To avoid being discovered by security systems, APT attackers often hide their operations using legitimate tools and processes, code obfuscation and anti-analysis measures.*

What are the main motives and targets of an APT attack?

The motives of advanced persistent threat actors vary. For example, attackers sponsored by nation states might target intellectual property (IP) or classified data to gain a competitive advantage in certain industries. Other target sectors often include power distribution and telecommunications utilities and other infrastructure systems, social media, media organizations, financial organizations, high tech and government agencies. Organized crime groups sponsor advanced persistent threats to gain information they can use to carry out criminal acts for financial gain.

Although APT attacks can be difficult to identify, data theft is never completely undetectable. However, the act of exfiltrating data from an organization might be the only clue defenders have that their networks are under attack. Cybersecurity professionals often focus on detecting anomalies in outbound data to see if the network has been the target of an APT attack.

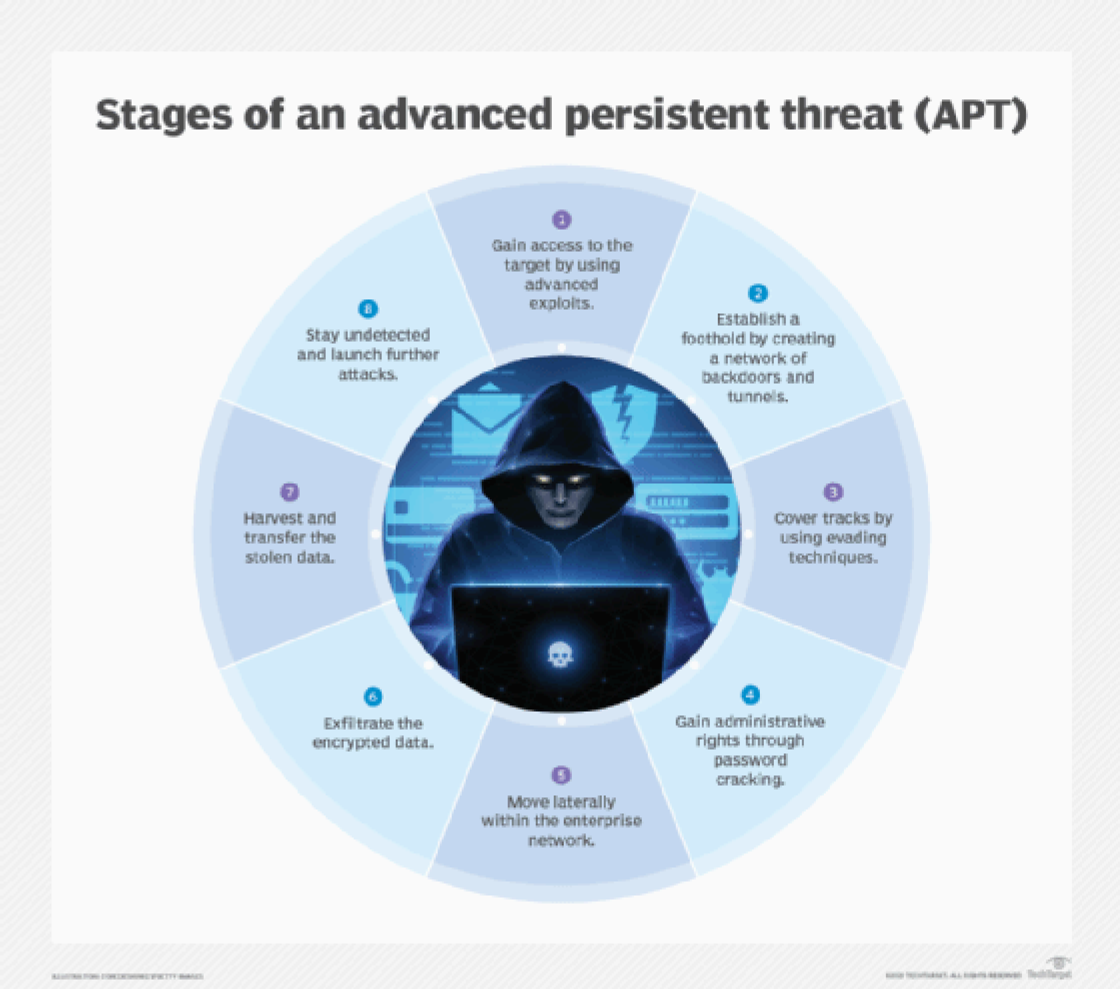
Stages of an APT attack

Attackers executing APTs typically take the following sequential approach to gain and maintain ongoing access to a target:

1. ***Gain access.*** *APT groups gain access to a target's network through the internet. Normally, they gain access by inserting malicious software into the target through spear phishing emails or via an application vulnerability.*
2. ***Establish a foothold.*** *After gaining access to the target, threat actors use their access to do further reconnaissance. They use the malware they've installed to create networks of backdoors and tunnels to move around unnoticed.*
3. ***Cover tracks.*** *APTs often use advanced malware techniques such as code rewriting to cover their tracks and evade detection.*
4. ***Gain even greater access.*** *Once inside the targeted network, APT actors use methods such as password cracking to gain*

administrative rights. This gives them more control of the system and even deeper levels of access.

5. ***Move laterally.*** *Once threat actors have breached their target systems, including gaining administrator rights, they can move around the enterprise network at will. They can also attempt to access other servers and other secure areas of the network.*
6. ***Stage the attack.*** *At this point, the hackers centralize, encrypt and compress the data so they can exfiltrate it.*
7. ***Take the data.*** *The attackers harvest the data and transfer it to their system.*
8. ***Remain until they're detected.*** *Cybercriminals will repeat this process for long periods of time until they're detected, or they can create a backdoor so they can access the system again later.*


Stages of an advanced persistent threat (APT)
1 Gain access to the target by using advanced exploits.
2 Establish a foothold by creating a network of backdoors and tunnels.
3 Cover tracks by using evading techniques.
4 Gain administrative rights through password cracking.
5 Move laterally within the enterprise network.
6 Exfiltrate the encrypted data.
7 Harvest and transfer the stolen data.
8 Stay undetected and launch further attacks.
TechTarget

An APT attack follows these general steps.

Examples of advanced persistent threats

APTs are usually assigned names by the organization that discovered them, though many advanced persistent threat attacks have been discovered by more than one researcher, so some are known by more than one name.

Advanced persistent threats have been detected since the early 2000s, and they date back as far as 2003 when China-based hackers ran the "Titan Rain" campaign against U.S. government targets to steal sensitive state secrets. The attackers targeted military data and launched APT attacks on the high-end systems of U.S. government agencies, including the National Aeronautics and Space Administration and the Federal Bureau of Investigation. Security analysts pointed to the Chinese People's Liberation Army as the source of the attacks.

Examples of advanced persistent threats include the following:

- ***Gelsemium** targeted a Southeast Asian government for six months between 2022 and 2023. The cyber espionage group responsible has been operational since 2014. They initially exploited their target by installing web shells to perform basic reconnaissance.*
- ***APT41** targeted the proprietary information of technology and manufacturing companies via malware, including digitally signed kernel-level rootkits. The Chinese state-linked group, also known as Winnti, targeted companies in East Asia, Western Europe and North America from at least 2019 to 2021.*
- ***APT37**, also known as Reaper, ScarCruft and Group123, is an advanced persistent threat linked to North Korea that's believed to have originated around 2012. APT37 has been connected to spear phishing attacks exploiting an Adobe Flash zero-day vulnerability.*

- ***APT34**, an advanced persistent threat group linked to Iran, was identified in 2017 by researchers at FireEye (now Trellix) but has been active since at least 2014. The threat group has targeted companies in the Middle East with recent attacks against financial, government, energy, chemical and telecommunications companies.*
- ***APT32**, a Vietnamese APT group also known as OceanLotus, SeaLotus and Cobalt Kitty has been active since at least 2014. It focuses on organizations in Southeast Asia, particularly those with ties to the region's politics or economy. APT32 has been involved in espionage operations, leading campaigns against firms in the private sector, media outlets and government institutions.*
- ***APT29**, the Russian advanced persistent threat group also known as Cozy Bear, has been linked to several attacks, including a 2015 spear phishing attack on the Pentagon, as well as the 2016 attacks on the Democratic National Committee.*
- ***APT28**, the Russian advanced persistent threat group also known as Fancy Bear, Pawn Storm, Sofacy Group and Sednit Gang, was identified in 2014 by researchers at Trend Micro. APT28 has been linked to attacks against military and government targets in Eastern Europe, including Ukraine and Georgia, as well as campaigns targeting the North Atlantic Treaty Organization and U.S. defense contractors.*
- ***The Sykipot APT malware family** exploited flaws in Adobe Reader and Acrobat. It was detected in 2006, and further attacks using the malware reportedly continued through 2013. Threat actors used the*

Sykipot malware family as part of a long-running series of cyber attacks, mainly targeting U.S. and UK organizations. The hackers used a spear phishing attack that included links and malicious attachments containing zero-day exploits in targeted emails.

- ***The GhostNet cyber espionage operation*** *was discovered in 2009. Executed from China, the attacks were initiated via spear phishing emails containing malicious attachments. The attacks compromised computers in more than 100 countries. The attackers focused on gaining access to the network devices of government ministries and embassies. These attacks allowed the hackers to control these compromised devices, turning them into listening and recording devices by remotely switching on their cameras and audio recording capabilities.*
- ***The Stuxnet worm*** *used to attack Iran's nuclear program was detected by cybersecurity researchers in 2010. Although Stuxnet isn't considered a cybersecurity threat today, it's still considered to be one of the most sophisticated pieces of malware ever detected. The malware targeted SCADA (supervisory control and data acquisition) systems and was spread with infected USB devices. The U.S. and Israel have both been linked to the development of Stuxnet. While neither nation has officially acknowledged its role in developing it, there have been unofficial confirmations that they were responsible for Stuxnet.*

Characteristics of advanced persistent threats

Advanced persistent threats often exhibit certain characteristics reflecting the high degree of coordination necessary to breach high-value targets.

Common characteristics of APTs include the following:

- ***Sequential.*** *Most APTs are carried out in multiple phases, reflecting the same basic sequence of gaining access, maintaining and expanding access, and attempting to remain undetected in the target network until the goals of the attack have been accomplished.*
- ***Multiple points of compromise.*** *Advanced persistent threats are also distinguished by their focus on establishing multiple points of compromise. APTs usually attempt to establish multiple points of entry to the targeted networks, which enables them to retain access even if the malicious activity is discovered and incident response is triggered, enabling cybersecurity defenders to close one compromise.*
- ***Specific goals and objectives.*** *APTs have specific goals and motives, which can vary depending on the actors involved. These goals could involve conducting espionage, influencing political processes or stealing confidential information, financial data or IP. They might also involve interfering with business operations.*
- ***Enhanced timeframe.*** *While conventional cyber attacks, such as ransomware, typically unfold within a relatively brief timeframe,*

lasting days or weeks at most, APT attacks can span across months or even years.

- ***Coordinated and well-resourced.*** *APTs are frequently carried out by threat actors with strong organizational and financial capabilities, such as state-sponsored, organized crime gangs or highly proficient hacker groups. They can create unique tools, carry out in-depth reconnaissance and plan intricate strikes.*
- ***Expensive to carry out.*** *The creation and proliferation of advanced persistent threats can cost millions of dollars. Large, well-funded companies and groups of cybercriminals frequently choose to use APT attacks, as they're the most financially demanding type of cybercrime.*
- ***Redundant points of entry.*** *Once an APT has infiltrated a network, it often establishes multiple connections to its home servers, enabling potential deployment of additional malware. This strategy ensures redundant entry points, mitigating the risk of closure by network administrators.*

Detecting advanced persistent threats

Advanced persistent threats have certain warning signs despite typically being hard to detect. An organization might notice certain symptoms after it has been targeted by an APT, including the following:

- *Unusual activity on user accounts.*

- *Extensive use of backdoor Trojan horse malware, a method that enables APTs to maintain access.*
- *Odd or uncharacteristic database activity, such as a sudden increase in database operations involving massive quantities of data.*
- *A sudden increase in targeted spear-phishing attempts.*
- *The presence of unusual data files or large clumps of files in unusual locations, which could indicate data that has been bundled into files ready to be exported to assist in the exfiltration process.*

Detecting anomalies in outbound data is perhaps the best way for cybersecurity professionals to determine if a network has been the target of an APT attack.

APT security measures

To avoid and mitigate APTs, security teams must develop comprehensive security strategies. Key security measures against APTs include the following:

- ***Patching network software and operating system vulnerabilities.*** *Patching vulnerabilities in network software and OSes as soon as possible helps prevent attackers from exploiting known weaknesses.*

- ***Securing remote connections.*** *Securing remote connections through encryption prevents unauthorized access to sites by thwarting potential intruders from exploiting these connections.*
- ***Filtering incoming emails.*** *Filtering incoming emails is a key step in the prevention of spam and phishing assaults on a network as it doesn't let any suspicious emails pass through the network.*
- ***Prompt logging on security events.*** *Logging security incidents as soon as they happen can improve allowlists and other security policies.*
- ***Real-time traffic monitoring.*** *As a recommended best practice, companies should keep an eye on inbound and outbound traffic within the perimeter of their network to stop backdoor installations and the extraction of stolen data.*
- ***Setting up web application firewalls (WAF).*** *Installing WAFs on network endpoints and edge networks can help protect web servers and web applications from infiltration.*