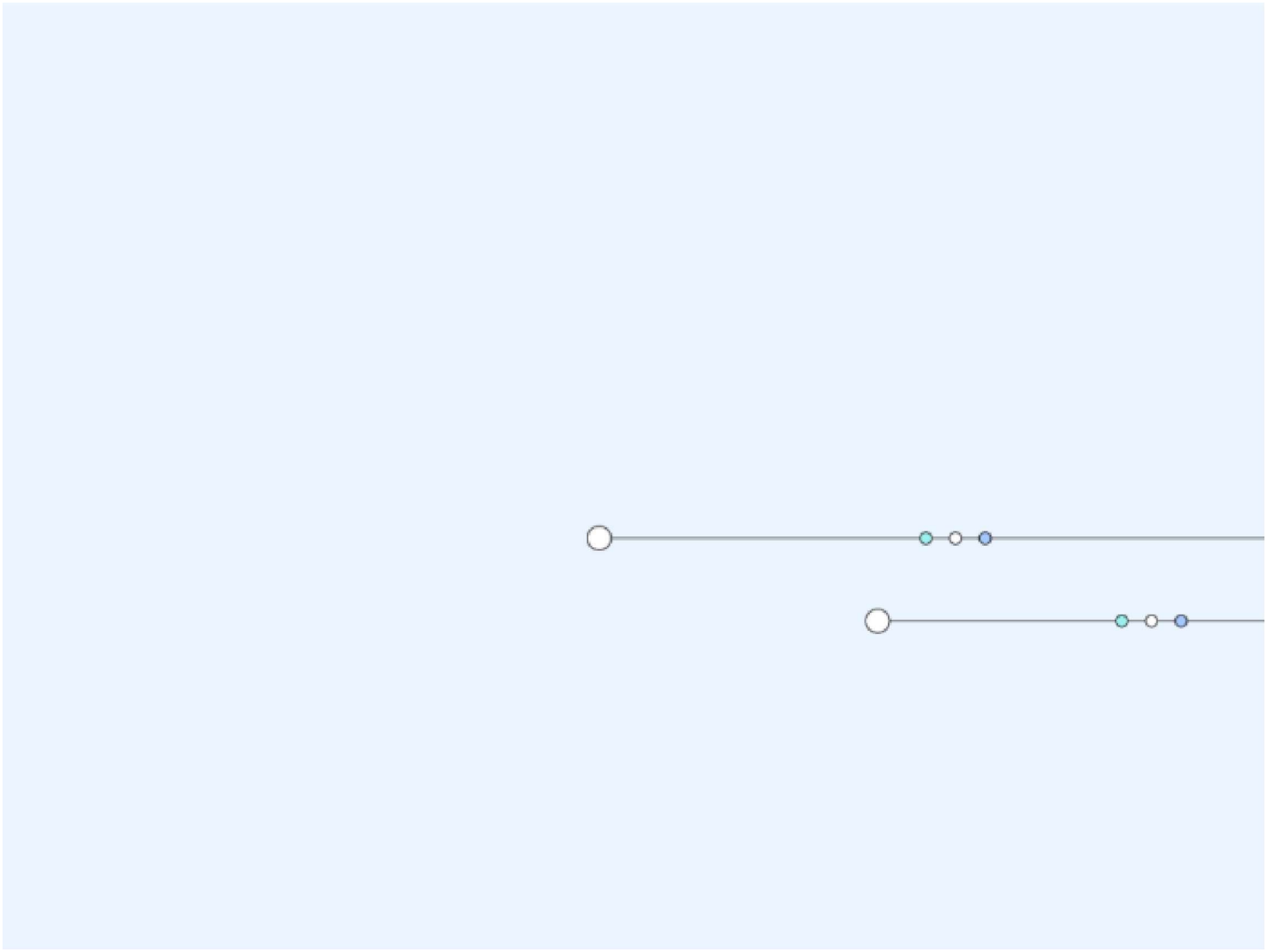
What are advanced persistent threats?



Overview

Stages of an APT attack

Common APT attack techniques

Examples of APT groups

Detecting an APT attack

Protecting against an APT attack

Products

Resources

Take the next step

Published: 3 April 2024

Contributors: Gregg Lindemulder, Amber Forrest

What are advanced persistent threats?

Advanced persistent threats (APT) are undetected cyberattacks designed to steal sensitive data, conduct cyber espionage or sabotage critical systems over a long period of time. Unlike other cyberthreats such as ransomware, the goal of an APT attack group is to remain unnoticed as it infiltrates and expands its presence across a target network.

State-sponsored teams of cybercriminals often execute APT attacks to access the sensitive information of other nation-states, or the intellectual property of large organizations. Although they may initially use traditional social engineering techniques, these threat actors are known for customizing advanced tools and methods to exploit the unique vulnerabilities of specific organizations. A successful APT attack may last months or even years.

Research

IBM X-Force Exchange

Explore global threat intelligence

Related content

Unpack key stats from the Cost of a Data Breach report

Stages of an APT attack

Infiltration

APT groups often gain initial access to their target network through social engineering and spear phishing. Using intelligence gathered from sources inside and outside an organization, APT attackers will create sophisticated spear phishing emails that convince executives or senior leaders to click on a malicious link. Attackers may also pursue other entry points and attack surfaces to penetrate the network. For instance, they may launch a zero-day attack on an unpatched vulnerability in a web application, or embed malware on a public website that employees are known to visit.

Exploration and expansion

After the initial intrusion, APT groups will explore and map the network to determine the next best steps for lateral movement across the organization. By installing a series of backdoors, which allow them to access the network from multiple entry points, they can continue to perform reconnaissance and install hidden malware. They may also attempt to crack passwords and gain administrative rights to secure areas where sensitive data resides. Most importantly, attackers will create a connection to an external command and control server for remote management of the hacked systems.

Exfiltration

To prepare for the first instance of data theft, APT groups will move the information they have collected over time to a centralized, secure location within the network. They may also encrypt and compress the data for easier exfiltration. Then, to distract security personnel and divert resources, they may stage a “white noise” event such as a Distributed Denial of Service (DDoS) attack. At this point, they are able to transfer the stolen data to an external server without detection.

Maintenance

APT groups may remain inside a breached network for an extended period or indefinitely, as they await new opportunities to stage an attack. During this time, they may maintain their hidden presence by rewriting code to conceal malware and installing rootkits that provide access to sensitive systems without detection. In some cases, they may remove evidence of the attack and leave the network entirely after they have achieved their objectives.

Common APT attack techniques

Social engineering
Using broadly distributed phishing emails, highly personalized spear phishing emails or other social manipulation tactics, APT groups convince users to click on malicious links or reveal information that grants access to protected systems.

Zero-day attacks
By deploying malicious shellcode that scans networks for unpatched software vulnerabilities, APT groups are able to exploit areas of weakness before IT administrators can react.

Supply chain attacks
APT groups may target the trusted business, technology or vendor partners of an organization to gain unauthorized access through shared software or hardware supply chains.

Rootkits
With the ability to provide hidden, backdoor access to protected systems, rootkits are a valuable tool for helping APT groups conceal and manage remote operations.

Command and control servers
Once APT groups gain a foothold in a breached network, they establish a connection to their own external servers to remotely manage the attack and exfiltrate sensitive data.

Other techniques
APT groups may use an array of other tools to expand and conceal their presence across a network such as worms, keylogging, bots, password cracking, spyware and code obfuscation.

Examples of APT groups

APT34 (Helix Kitten)
Known for its remarkably convincing and well-researched spear phishing emails, Helix Kitten allegedly operates under the supervision of the government of Iran. The group primarily targets companies in the Middle East across industries such as aerospace, telecommunications, financial services, energy, chemical and hospitality. Analysts believe these attacks are intended to benefit Iran's economic, military and political interests.

APT41 (Wicked Panda)
Wicked Panda is a notorious and prolific China-based APT group with alleged ties to the Chinese Ministry of State Security and the Chinese Communist Party. In addition to conducting cyber espionage, members of this group are also known for attacking companies for financial gain. They are believed to be responsible for hacking into healthcare supply chains, stealing sensitive data from biotech firms, and the theft of COVID-19 relief payments in the United States.

Stuxnet
Stuxnet is a computer worm that was used to disrupt Iran's nuclear program by targeting supervisory control and data acquisition (SCADA) systems. Although it is no longer active today, it was considered to be a powerfully effective threat when it was discovered in 2010, causing significant damage to its target. Analysts believe Stuxnet was co-developed by the United States and Israel, although neither nation has openly admitted responsibility.

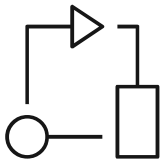
Lazarus Group
The Lazarus Group is a North Korea-based APT group believed to be responsible for the theft of hundreds of millions of dollars in virtual currency. According to the U.S. Department of Justice, the crimes are part of a strategy to undermine global cybersecurity and generate revenue for the North Korean government. In 2023, the U.S. FBI accused the Lazarus Group of stealing USD 41 million in virtual currency from an online casino.

Detecting an APT attack

Because APT attacks are designed to mimic normal network operations, they can be difficult to detect. Experts recommend several questions that security teams should ask if they suspect they have been targeted.

Is there unusual activity on user accounts?
APT threat actors target high-value user accounts with privileged access to sensitive information. These accounts may experience unusually high volumes of log-ons during an attack. And because APT groups often operate in different time zones, these log-ons may occur late at night. Organizations may use tools such as endpoint detection and response (EDR) or user and entity behavior analytics (UEBA) to analyze and identify unusual or suspicious activity on user accounts.

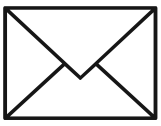
Is there a significant increase in backdoor Trojans?
Most IT environments experience backdoor Trojans, but during an APT attack their presence may become widespread. APT groups rely on backdoor Trojans as a backup for re-entry to compromised systems after they have been breached.



Is there unusual data transfer activity?
A significant deviation from the normal baseline of data transfer activity may suggest an APT attack. This could include an abrupt increase in database operations and the internal or external transfer of massive amounts of information. Tools that monitor

and analyze event logs from data sources, such as security information and event management (SIEM) or network detection and response (NDR), can be helpful for flagging these incidents.

Has data been aggregated and moved to an unusual location? APT groups commonly amass large amounts of data from across a network, and move that information to a central location before exfiltration. Large bundles of data in an odd location, especially if it is in a compressed format, may indicate an APT attack.



Have select executives received spear phishing emails? Spear phishing attacks that target a small number of high-level leaders are a common tactic among APT groups. These emails often contain confidential information and use document formats such as Microsoft Word or Adobe Acrobat PDF to launch malicious software. File integrity monitoring (FIM) tools can help organizations detect if critical IT assets have been tampered with due to malware embedded in spear phishing emails.

Protecting against an APT attack

There are security measures organizations can take to mitigate the risk of APT hackers gaining unauthorized access to their systems. Because APT groups continually adapt new methods for each attack vector, experts recommend a broad approach that combines multiple security solutions and strategies including:

- **Patching software** to safeguard network and operating system vulnerabilities against zero-day exploits.
- **Monitoring network traffic** in real time to spot malicious activity such as the installation of backdoors or the exfiltration of stolen data.
- **Using web application firewalls** on network endpoints that filter traffic between web applications and the internet to prevent incoming attacks.
- **Implementing strict access controls** that prevent unauthorized users from accessing sensitive or high-level systems and data.
- **Conducting penetration testing** to identify areas of weakness and vulnerabilities that APT groups could exploit during an attack.
- **Leveraging threat intelligence** to better understand the lifecycle of an APT attack and plan for an effective incident response if it appears one is underway.

Related solutions

Vulnerability management services

Identify, prioritize and manage the remediation of flaws that could expose your most-critical assets.

Explore vulnerability management services →

Resources

Report

IBM X-Force Threat Intelligence Index

Get actionable insights to help you understand how threat actors are waging attacks—and

Read the report

Related topic

What is threat management?

Threat management is a process that is used by cybersecurity professionals to prevent

Learn more

Related topic

What is a threat actor?

Threat actors, also known as cyberthreat actors or malicious actors, are individuals or groups that

Learn more

Take the next step

IBM cybersecurity services deliver advisory, integration and managed security services and offensive and defensive capabilities. We combine a global team of experts with proprietary and partner technology to co-create tailored security programs that manage risk.

Explore cybersecurity services →

Subscribe to the Think Newsletter →