WHAT ARE APTS? ADVANCED PERSISTENT THREATS EXPLAINED



Today, the global economy is heavily centered on digital technology—and the value of data held by individuals and entities is now valued at a high premium.

As a result, cybercrime has become more and more sophisticated, especially where organized groups invest in skills, tools, and processes to take down targets and monetize the looted information. Be it government agencies, research institutions, or corporates, wherever valuable data can be found, these groups take their time to:

- Investigate, infiltrate, and extract data
- Extort a ransom
- Damage IT systems

This type of long-term attack by specialist groups is called an advanced persistent threat (APT).

A report by ENISA, the EU Agency for Cybersecurity, showed that attacks conducted by APTs on EU institutions, bodies, and agencies increased by 30% in 2021. Just recently, the Red Cross detailed such an attack where personal data belonging to over 500,000 people was compromised. The attack was discovered on 18th January, but it was determined that the intrusion occurred on 9th November.

In this article, let's do a deep dive on APTs including who they are and how they structure their attacks, and, more importantly, how to protect ourselves from such entities.

What is an APT?

An APT is a calculated network attack on any organization. These threats occur when a hacker, or group of hackers, establishes a foothold inside an enterprise network. APTs go undetected for prolonged periods of time, allowing for sensitive data to be mined.

The term APT references the type of attack—multi-stage in nature—but over time has been used to characterize the groups or the tools in use. The primary goal of APTs is data theft, but there is increasing evidence of other objectives such as:

- Ransomware
- Espionage
- Systems disruption
- Crypto mining

So, who is conducting APTs? The characteristics of such attacks indicate that the main players are well-funded entities who have the time, muscle, and laser-focused attention to get to their goal.

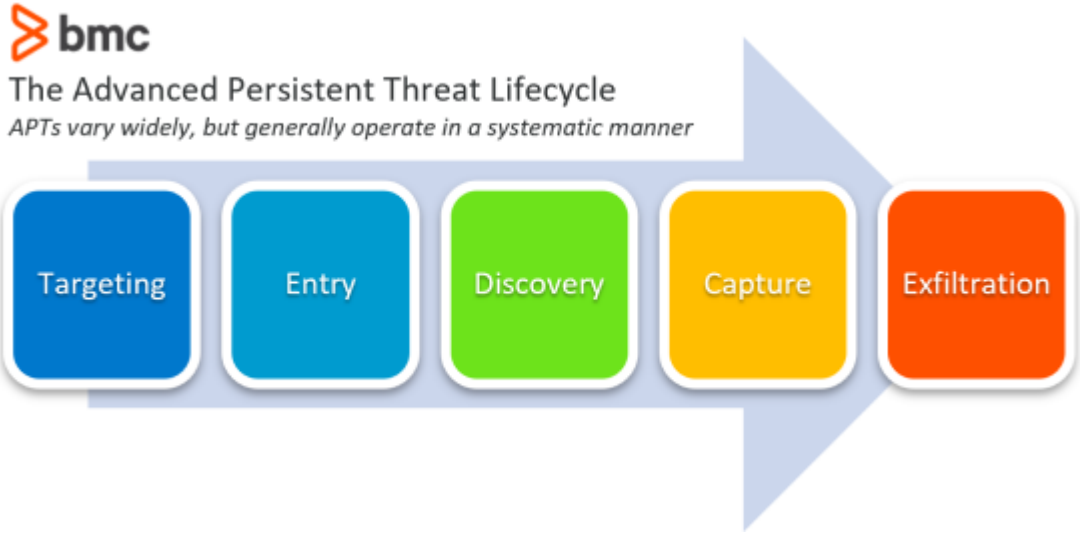
There is significant evidence that some of these groups are state sponsored entities, like APT27 and Winnti that are alleged to be Chinese sponsored, with the former recently flagged by the German government for attacks on government agencies. The US CISA has also raised an alert about Iranian sponsored APTs exploiting Fortinet and Microsoft Exchange vulnerabilities.

Trend Micro's 2021 mid-year cybersecurity report listed the following groups (with interesting coined names) actively involved in ATP attacks:

- Team TNT targeted AWS credentials and Kubernetes clusters for crypto mining.
- Water Pamola targeted e-commerce shops in Japan with XSS script attacks.
- Earth Wendigo targeted Taiwan institutions webmail with malicious JavaScript backdoors.
- Earth Vetala targeted institutions in the Middle East using remote access tools to distribute malicious utilities.
- Iron Tiger targeted institutions in Southeast Asia using a SysUpdate malware variant.

Lifecycle & characteristics of an APT

While no two APTs are the same, in general, advanced persistent threats operate in a systematic manner. The lifecycle of an APT happens in five stages, as listed below:



Stage 1: Targeting/Reconnaissance

Initially, an enterprise is targeted by hackers who seek to accomplish a singular agenda. Infiltrating occurs through identified weaknesses in the network, web assets, or other resources that hackers can gain access to.

Attackers will also use information from the internet and social media to identify contacts of potential victims to be targeted through social engineering attacks such as spear phishing.

Stage 2: Entry

Hackers gain access using SQL injections, RFIs, or implementing phishing scams that enable entry via user access points. Exploiting zero-day vulnerabilities in unpatched systems is fast becoming the go-to entry method for most APTs:

- The Red Cross attack involved exploiting an unpatched critical vulnerability in Zoho ManageEngine ADSelfService Plus (CVE-2021-40539).
- The ATP attack on a U.S. municipal government webserver involved exploitation of vulnerabilities on a Fortigate appliance, and the creation of an account with the username "elie" to enable further malicious activity.

Once inside a network, hackers will often create a backdoor by uploading malware that allows repeatable entry. In Germany, APT27 used the malware variant HyperBro remote access trojan to backdoor their networks from compromised commercial companies. Additional attacks may be used to create a smoke screen that allows hackers time to gain access undetected.

(Understand how vulnerabilities work.)

Stage 3: Discovery

Entry into the system is the first milestone for a hacker launching a calculated APT attack. The next involves taking steps to avoid detection. To do this, hackers will map out the organization's infrastructure and launch additional attacks to the system, geared at gaining access to user accounts higher in the hierarchy. The higher in the hierarchy a malicious cyber attacker can get the better the access to sensitive information.

Post-exploitation activities identified in the Red Cross attack included compromising administrator credentials, conducting lateral movement, and exfiltrating registry hives and Active Directory files.

Stage 4: Capture

An infrastructure left vulnerable from multiple cyber-attacks is easier to move around in undetected. Under these conditions, hackers begin capturing data over an extended period of time. Capture can also include

- Building stable remote control
- Establishing communication with command-and-control centers

The hackers involved in the Red Cross attack deployed offensive security tools which allowed them to disguise themselves as legitimate users or administrators.

Stage 5: Data exfiltration

Once identified, infiltrators can deploy malware extraction tools to steal desired data. Usually this means creating "white noise attacks" to cover cyber attackers who want to mask their intentions. They also mask their entry point, leaving it open for further attacks.

An alternative is ransomware, where the ATP will encrypt the victim's enterprise data and demand payment in cryptocurrency in exchange for decryption keys.

Identifying APTs: What to look for

If an enterprise business has been hit with an APT, it can be hours, days, or longer before they discover the problem. But time is of the essence when it comes to protecting your organization.

Monitoring your infrastructure for these signs can help you stay ahead of hackers who try to establish a foothold in your network:

Increase in late-night logging

Are employees suddenly logging in late at night? This could be a warning sign that your system has been exposed to cyber attackers gaining access to your employee's log ins at night when no one is around to stop them.

What to do: If enterprise business leaders see this kind of activity, it should be a red flag to further investigate for vulnerabilities.

Trojans are prolific in the network

When hackers access a computer in a network, they often install a trojan which gives them total control over that machine, even after passwords have been updated for security.

What to do: If enterprise organizations have a network full of trojans, they should consider the possibility the network is under attack from an APT.

Unexpected data bundles

One way cyber attackers move data is by putting large amounts of data into bundles before shipping it out of the system.

What to do: Identifying unexpected bundles of gigabytes of data is a good indicator to check your enterprise infrastructure.

Unexpected data flows

One way to spot an APT is to look for unexpected flows of data. These could be computer to computer, server to server, in or out of network. In order to identify whether an information flow is unauthorized or unexpected, you have to know what's reasonably expected within your current infrastructure.

What to do: Define reasonable expectations for data flows and monitor for discrepancies.

Final thoughts

Advanced persistent threats are complicated, calculated, long-game attacks that can have devastating effects on an enterprise business and, unfortunately, cannot be easily predicted. However, enterprise organizations don't have to be at the mercy of APTs. You can implement strategies that include:

- Continuous automated patching
- Advanced endpoint detection and response monitoring systems
- Multi-factor authentication and strong password protection mechanisms
- Response planning to create a big picture of what to do if a breach occurs

Deploying AI and ML based security solutions can be highly effective in detecting anomalous behavior, which is one of the hallmarks of an APT attack.

Related reading

- BMC Security & Compliance Blog
- AI Cyberattacks & How They Work, Explained
- Introduction to Vulnerability Management
- Risk Assessment vs Vulnerability Assessment: How To Use Both
- What is CVE? Common Vulnerabilities and Exposures Explained
- Business Continuity Planning: How To Create & Maintain BCPs