**What is an Advanced Persistent Threat (APT) Attack?** An**APT**, or **Advanced Persistent Threat** is covert and sustained cyber-attack in which an attacker uses sophisticated methods to establish undetected presence within the network for a significant period after gaining unauthorized access to a computer network or a system.

This article is focused on giving you an understanding about APT, its life cycle, and how to protect against APT attacks.

The primary goal of the attacker is data theft but there are some other objectives of APT according to the recent evidence of APT attacks such as ransomware, crypto-mining, system disruption and espionage.

By segregating the word Advanced Persistent Threat into the following terms, the idea of APT can clearly understand as follows.

**ADVANCED** Although APT attacks use sophisticated operations to attack there are some unsophisticated methods such as social engineering, zero-day vulnerabilities and phishing attacks used with multiple other tools and strategies to gain unauthorized access to target system. After gaining access to the system, the attackers' main objective is to exploit security weakness and wait for an opportunity to move forward with the attack. The term advanced is used as the attacker harness latest advanced techniques and multiple tools to find system vulnerabilities.

PERSISTENT For an advanced attack, there is a need for patience and wait for the opportunity to intrude to the system. APT attacks sometimes take months to many years to initialize the attack. During this time the attacker will spend time in network while observing and learning the patterns and defense tactics. Therefore, persistent means long term target access with dormant activity.

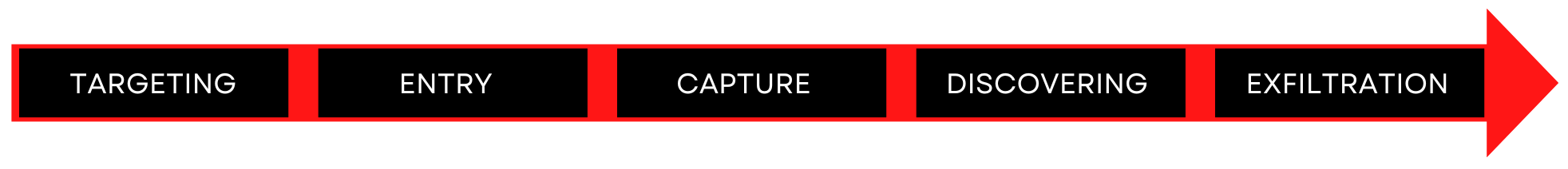
**THREAT** APT attacks consider as a threat due to the type of target by the attacker. Here the attacker targets a high- value network system other than a single actor scheme. An organization with data storage, communication and network facilities are vulnerable to APT attacks. This includes government organizations, healthcare facilities and other manufacturing industries. The attackers who initialize APT attack's main goal is to cause a larger damage such as economic disaster or political chaos.

Further, APT attack can cause a serious security threat to the entire enterprise network, leading to a consequential loss of:

* Intellectual property (IP) theft
* Personally identifiable information (PII) theft
* Sensitive data breach and destruction
* Accessing critical communications

These attacks carried out by highly skilled, well-funded group such as government cyber warfare teams or terrorist groups. APT attacks consider as high threat attacks due to the nature of the attack which includes a long-term plan.

**Lifecycle & characteristics of an APT**



Advanced Persistent Threat Lifecycle

**Stage 1: Targeting/Reconnaissance** Attackers use information from the internet and social media to identify contacts of target victims through social engineering attacks such as spear phishing. Then the infiltrating occurs through identified weaknesses of the web application, the network or other resources that hackers can gain access to.

**Stage 2: Entry**

To gain unauthorized user access to the target system, the attacker use SQL injections, RFIs, or implement phishing scams that enable entry via user access points. Attackers can use zero-day vulnerabilities in unpatched systems to gain fast access to unpatched systems.

* The Red Cross attack involved exploiting an unpatched critical vulnerability in Zoho ManageEngine ADSelfService Plus (CVE-2021-40539).

After entering into the system, attacker will create a backdoor by uploading malware that allows repeatable entry. In Germany, APT27 used the HyperBro malware, remote access trojan to backdoor their networks from compromised commercial companies. Additional attacks can use to create a smoke screen that allows attackers to gain access to the system undetected.

**Stage 3: Discovery** After entering into the system, the next step of the APT attack is to avoid detection. Here attackers will map out the organization’s infrastructure and launch additional attacks to gain high level user access to get sensitive information.

**Stage 4: Capture** An infrastructure left vulnerable from multiple cyber-attacks is easier to move around in undetected. Under these conditions, attackers start capturing data over an extended period of time. Capture can also include:

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

The attackers involved in the Red Cross attack used offensive security tools which allowed them to disguise themselves as legitimate users or administrators of the system.

**Stage 5: Data exfiltration** After identified the target data, the final step is to steal desired data by using malware extraction tools. They use the method called “white noise attacks” to cover cyber attackers to mask their true intentions. They also mask their entry point, leaving it open for further attacks.

An alternative attack method is ransomware, where the ATP will encrypt the victim’s data and demand for payment to decrypt their data.

**How do you Protect Against APT Attacks?** Many organizations use different tactics to protect against APT attacks using different cybersecurity and intelligence solutions. Here are few example tactics:

* **Use Sensor Coverage -**Organizations can provide their defenders with full visibility across their environment to avoid blind spots that can be an easy target for cyber threats and attackers to access the system without noticing.
* **Leverage Technical Intelligence -**Use of indicators of compromise (IOCs) and consume them into a SIEM for data enrichment purposes helps to increase technical intelligence. When conducting event correlation, technical intelligence helps to highlight events on the network which reduce the risk of occurring APT attacks undetected.
* **Application of Web Application Firewall (WAF) -** It helps to protect organizations at the application level by filtering, monitoring and analyzing HTTP and HTTPS traffic between the web application and the internet.
* **Use of Threat Intelligence -**It helps for threat actor profiling, campaign tracking and malware family tracking as it is more important to understand the context of an attack rather than just knowing an attack itself happened.
* **Use of Threat Hunting -** Many organizations use 24/7, managed, human based threat hunting to monitor their cybersecurity policies already in place.

**Why would someone launch an APT?** A successful advanced persistent threat (APT) is extremely effective and beneficial to the attacker.

For nation states, there are significant political motivations, such as military intelligence, cause of economic disaster and reduce terrorist attacks. Examples include the Titan Rain, Ghostnet and Stuxnet attacks.

For smaller groups, APTs can lead to significant competitive advantages and lucrative payouts.

The goals of APTs fall into four general categories:

* Cyber Espionage, including theft of intellectual property or state secrets.
* e-Crime for financial gain
* Hacktivism
* Destruction

Always APT attacks will cause harm to the victims' party while the attacker gains access to the unauthorized data. Therefore, as cybersecurity professionals we have to protect the privacy of each individual through defensive mechanisms as well as awareness programs for employees for organizations.

**Recent APT Campaigns and Targets**:

1. APT29 (Cozy Bear) and APT28 (Fancy Bear): These two Russian state-sponsored APT groups gained global attention for their involvement in various high-profile campaigns. Notable targets include government agencies, political organizations, and critical infrastructure sectors.
2. APT40 (Periscope): Operating out of China, APT40 has been associated with cyber espionage campaigns targeting maritime-related organizations, particularly in the South China Sea region. Their focus includes the theft of sensitive information and intellectual property.
3. APT33 (Elfin): This Iranian-linked APT group has been involved in targeting aerospace, energy, and petrochemical industries, particularly in the Middle East. Their campaigns have included destructive attacks and espionage activities.

**APT examples**

APTs can be traced back to the 1980s, and they disturb the digital world on a greater scale. Moreover, these attacks have been generally organized by groups associated with nation-states and target highly valuable information. The following are 3 notable examples of advanced persistent threats.

**GhostNet**

GhostNet is considered to be one of the most sophisticated and oldest APTs the digital has seen so far. It was first discovered in March of 2009. Its control infrastructure was reported to have been located [**largely in China**](https://www.itbusinessedge.com/slideshows/the-most-famous-advanced-persistent-threats-in-history-07.html), and this attack was directed against the Tibetan community, however, the Chinese government has denied the fact.

The GhostNet attacks were executed by spear-phishing emails containing malicious downloadable files that loaded a Trojan horse on the user’s system, allowing the execution of commands from a remote command and control system, which downloaded malware to take full control of the infiltrated system.

The malware had the ability to use audio as well as video recording devices to monitor the locations housing the compromised computers. GhostNet was reported to have compromised the devices of political, economic, and media targets in nearly 103 countries, including the embassies of India, South Korea, Indonesia, Romania, and others. The Asian Development Bank and [ministries of foreign affairs](https://resources.infosecinstitute.com/ghostnet-part-i/#gref) of Bangladesh, Brunei, Indonesia, Iran, Latvia, Philippines were also among the victims.

**Deep Panda**

Deep Panda is believed to be a Chinese state-sponsored advanced cyber intrusion group to target several critical industries, such as government, defense, legal, financial, and telecommunications, for espionage purposes. [**CrowdStrike**](https://www.crowdstrike.com/?utm_expid=.XfysNxyCSV2dpcFrQWQESw.0&utm_referrer=https%3A%2F%2Fwww.google.com%2F), a cybersecurity technology company, stated that Deep Panda’s attack efforts were highly sophisticated and[**reflective of the status quo**](https://www.infosecurity-magazine.com/news/deep-panda-shifts-cyber-spying/) for cyber spying.

The main objective of this group was to maintain and sell access to compromised environments. Deep Panda was one of many hacking groups that Western cyber security organizations have accused of hacking into the United States and other countries’ networks and stealing government and defense files.

**Helix Kitten**

Helix Kitten is believed to be an Iran-based adversary group, and this group has been operational since 2014. Its major targets included organizations in aerospace, energy, financial, government, hospitality, and telecommunications, mostly in the Middle East. This advanced group has utilized perfectly structured spear-phishing messages that were so relevant to targeted users.

As regards the technicalities, this group was most commonly associated with [a custom PowerShell](https://www.wired.com/story/apt-34-iranian-hackers-critical-infrastructure-companies/) implant known as Helminth. The Helminth implant is routinely delivered via macro-enabled Microsoft Excel files demanding user interaction to implement an obfuscated Visual Basic Script. In fact, this is a highly multi-faceted approach: the group made many modifications, downloaded new malware, then manipulated the memory.

**APT attack lifecycle**

A typical APT life cycle is divided into [**4 phases**](https://pdfs.semanticscholar.org/310d/9b72a7e84f44fca66bbf3a9f25ce4f87a3d4.pdf): Reconnaissance, Initial compromise, creating foothold, and data exfiltration.  
  
**Reconnaissance** enables to discover the effective points of attack, assess target susceptibility, and the people within the organization who can expedite security breaches.

During the **initial compromise phase,** the attacker actually makes it inside the perimeter and obtains access. Although there are numerous ways to compromise a host, it has been done through the delivery of custom-written malware via a spear-phishing campaign. The spear-phishing attempts are usually sophisticated enough to make sure that the emails look legit for the target to click on the attachments or the hyperlinks.

Once a target has been compromised, the APT must guarantee that access is secured. The main goal in this phase is to expand the footprint of the initial compromise to ensure that even if one or more of the breaches is discovered, access is maintained.

Lastly, **data exfiltration** is the final phase of an APT life cycle. In this stage target information is detected, acquired, and moved out of the environment into the hands of the intruder. Often the data is packaged into an encrypted set of RAR files. When the attackers accomplish their goal, they cover their traces, deleting signs of their existence and any information that might enable them for finding the source of the attack.