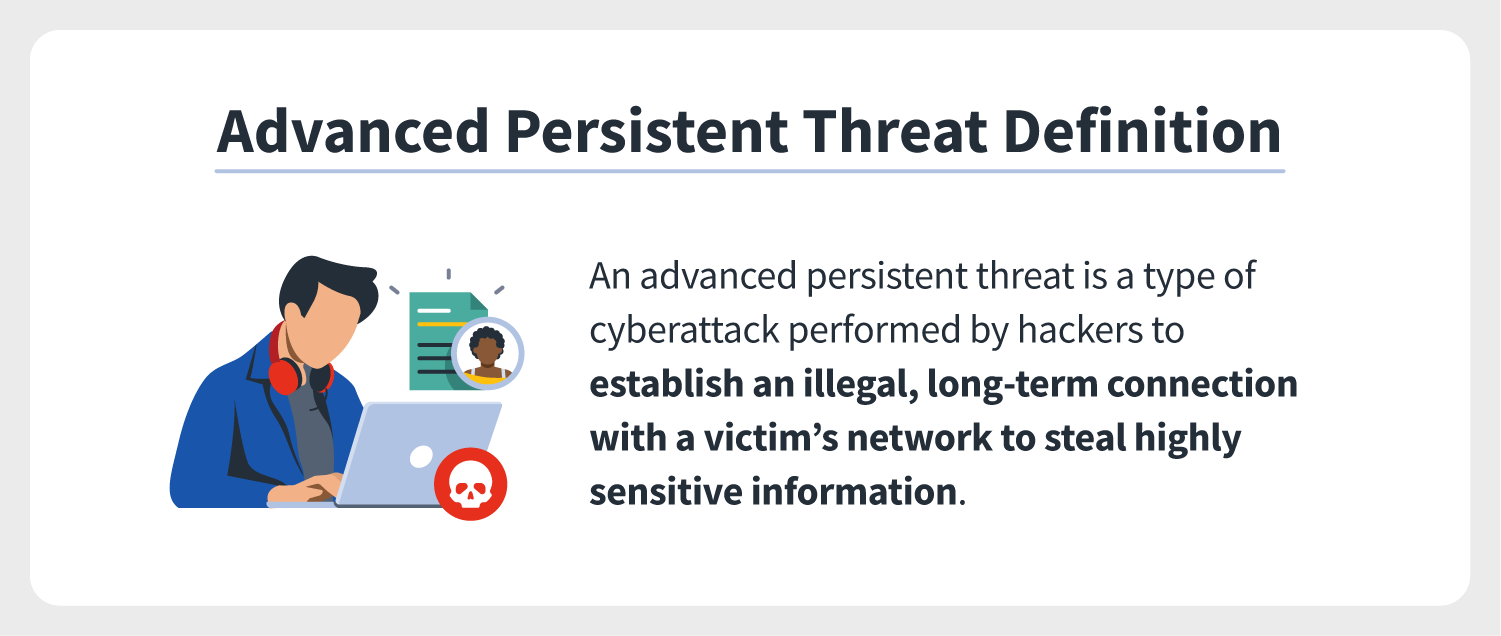
**Team Leader: TUSHAR**

**Member: SHREYA SHREE**

**GROUP PROJECT IN ADVANCE PERSISTENT THREAT (APT)**

**Introduction:** The [**cybersecurity**](https://www.geeksforgeeks.org/cyber-security-types-and-importance/)experts to be in alert all time. It is a kind of attack employed by the attacker by using a range of techniques, It is basically done by the attacker to steal valuable data and more. These attacks are being witnessed in major business sectors with some specific goals that are stealing data and so on.

**Advanced persistent threat:**

* The attacker/intruder gains access to the network and stays for a longer period of time. The **Goal** of the advanced persistent threat is to maintain access and to get data as much as possible.
* When the attackers are using the Advanced Persistent Threat, the targets are chosen carefully, and they are properly researched. To execute the APT, the attacker requires more resources.

**Advanced persistent threat is not like any traditional threat, they differ from that :**

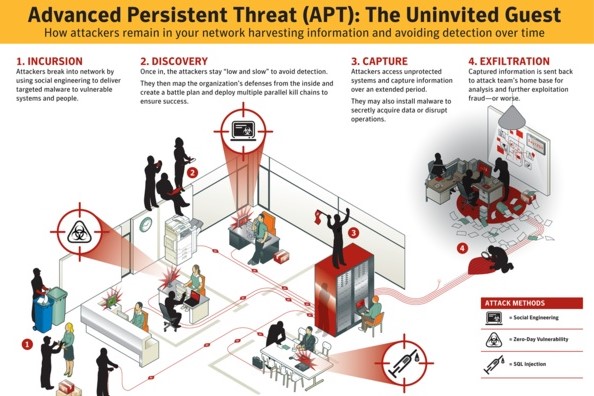
* They are more complicated.
* When the network gets infiltrated by the attacker, they stay for a longer period of time to get data as much as possible.

The attacker may have accessed the network, but there is a high chance of getting detected. So to maintain access for a longer period of time, the attacker tends to use **some advanced methods** rewriting malicious code and other.

**Note :**Advanced Persistent Threat is difficult to identify. This is why cybersecurity professionals always observe if there is any problem or if the network has become the target of an APT attack.

**Works :**  
There are some steps that the attacker does to gain access and maintain access on the network which are as follows :

1. **Gain access :**  
   The attackers can gain access through the network. This is done through spear-phishing email or other methods where the attacker’s main intention is to insert the malicious software into the target network.
2. **Broadening its access:**  
   When the access part is done by the attacker, they start exploiting the malware. This exploiting of malware makes the attacker move around without even getting detected.
3. **Gaining more access :**  
   When the attacker has gained access to the network, they may use some ways like password cracking to get the administrative rights. This will allow the attacker to get more control of the system and get access at a deeper level.
4. **Move at will :**  
   When the attacker has breached all the system and got the administrative rights they can move around.
5. **Harvesting of data :**  
   When the attackers are in the system, they start harvesting the data and store those data on their own system. They can remain in the system for a longer period of time until they are detected.

****

**APT Attack:**

An advanced persistent threat (APT) is a cyberattack in which an intruder gains and maintains a long-term presence within a network. The consequences of an APT attack are vast and include:

* [**Loss of data**](https://phoenixnap.com/blog/data-loss-prevention-best-practices) and intellectual property.
* Infrastructure sabotage.
* Service outage.

APTs are multi-stage attacks that take weeks to set up and last for months or even years. An APT is different from [**common cyberattacks**](https://phoenixnap.com/blog/cyber-security-attack-types) in four critical ways:

* An APT is more complex than a usual online threat. Attacks require full-time teams to maintain a hidden presence in the target network.
* APTs are not hit-and-run attacks. Once hackers access a network, their goal is to remain inside for as long as possible.
* An APT is mostly a manual attack that does not rely on automation.
* APTs are not a threat to a large pool of targets. Attacks go after a specific company, so each breach has a custom plan that fits only the target’s defenses.

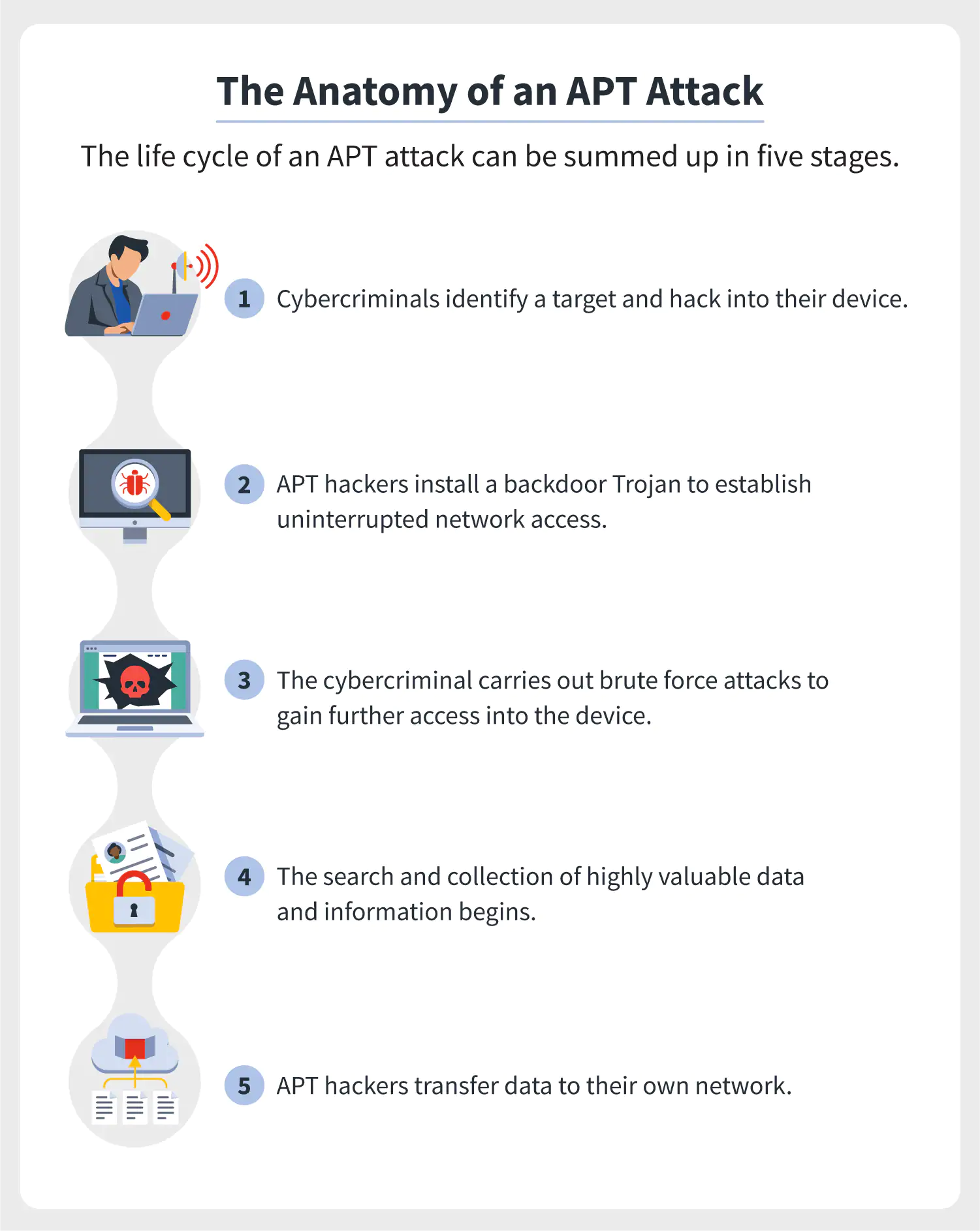
An APT attack requires a great deal of effort and resources. Hackers typically go after high-value targets, such as enterprises and corporations. APT attackers frequently target small firms in the supply chain of larger organizations.

Hackers use less defended companies as an entry point, so businesses of all sizes must know how to recognize an APT attack.

**Objectives:**

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. It is usually by a group of hackers and runs for a long period of time. An APT attack is designed to achieve a specific objective such as sabotage, corporate espionage, theft of intellectual property or exfiltration of personal financial data.

**Life Cycle:** 

**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.

**Characteristics:**

1. **Advanced Techniques** – APTs often use sophisticated techniques such as social engineering, zero-day exploits, and custom malware to gain access and maintain persistence in a network.
2. **Persistence** – APTs are designed to remain undetected for long periods of time, allowing attackers to maintain access and continue to steal data or perform other malicious activities.
3. **Targeted** – APTs are targeted attacks, with attackers carefully selecting their targets based on their value and potential for success.
4. **Data Exfiltration** – APTs are designed to steal sensitive data, which is then exfiltrated out of the targeted network to the attacker’s system.

**Detection the Apt :**

1. It can be some unusual activity on user accounts.
2. It can be some unusual data files present in the system.

**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

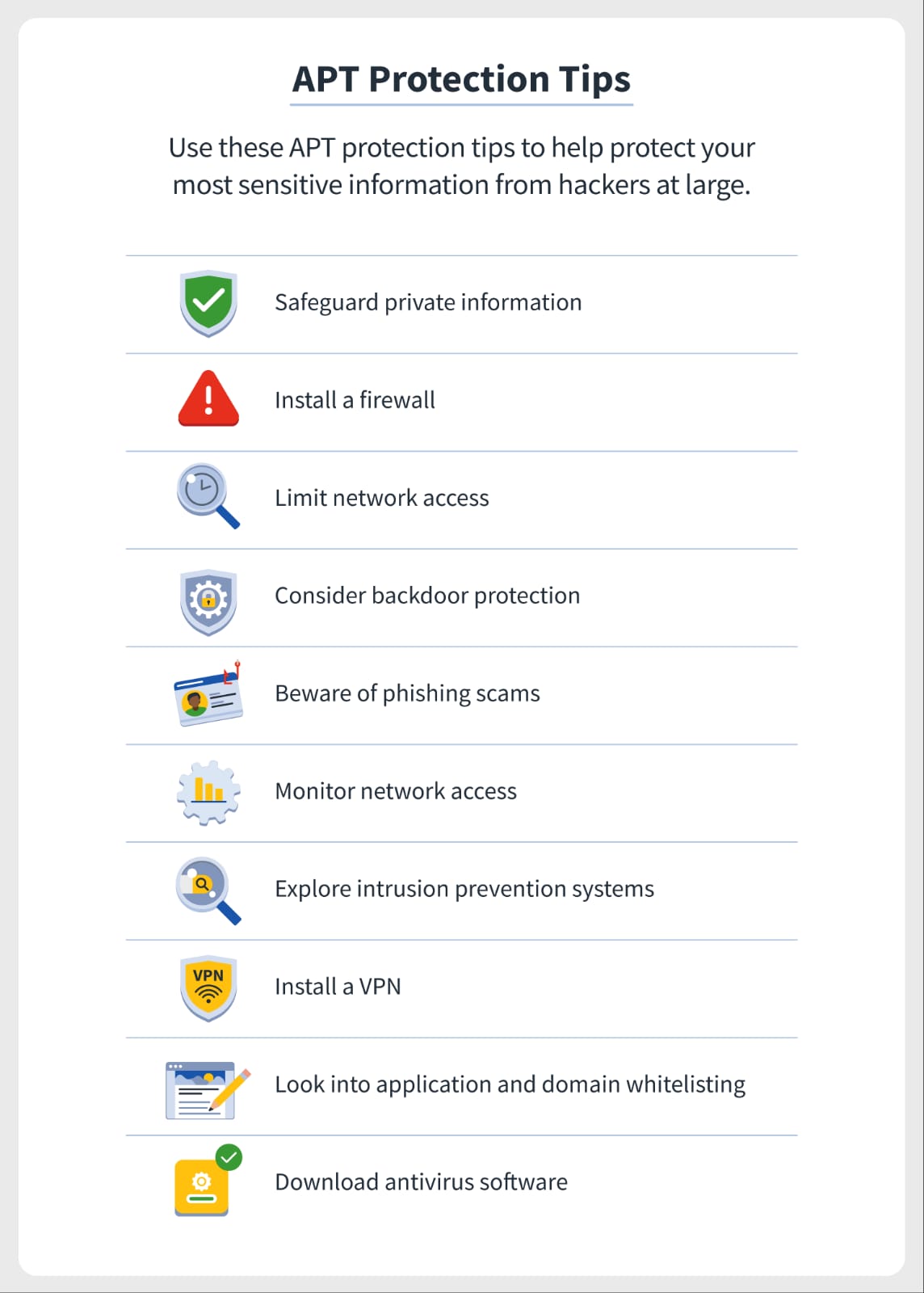
**Protected from Apt :**

Many organizations use different tactics to protect against APT attacks using different cybersecurity and intelligence solutions. Here are few example tactics:

There must be a firewall in the system. It will act as the first layer of defense in the Advanced Persistent Threat.

An antivirus should be installed in the system.

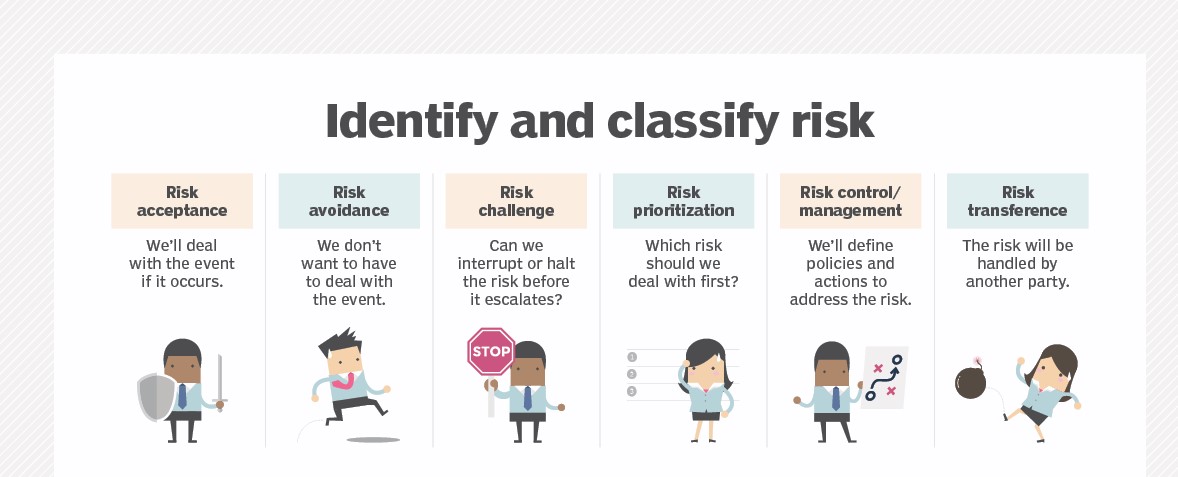
One should also enable email protection.



* **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.
* **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.
* **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.



**Mitigation strategies:**





**Emerging trends:**

**What are the trends in cybersecurity 2023?**

In 2023, one of the cybersecurity trends is expected to be the increased focus on users as an attack surface. Cyber attackers will continue to target an organization's user base by using tactics like phishing, social engineering, and other methods to gain unauthorized access.

One of the biggest trends in the future of cybersecurity is the use of artificial intelligence (AI) and machine learning (ML) technologies. AI and ML algorithms are able to analyze large amounts of data and detect patterns and anomalies that may indicate a potential threat.