ADVANCED PERSISTENT THREATS – The biggest threat to cyber safety

Advanced persistent threats (APTs) are threats that the high skilled hackers use latest and sophisticated methods to enter any organization and attempts to exfiltrate valuable and sensitive data from the company.

Advanced persistent threats are very hard to detect and the APTs lasts for many months in average and can cause much damage to the company targeted in terms of company specific sensitive data and trade secrets.

Typically, APT attacks target organizations in sectors such as national defense, manufacturing, and the financial industry, as they deal with high-value information, including intellectual property, military plans, and other government and corporate data.

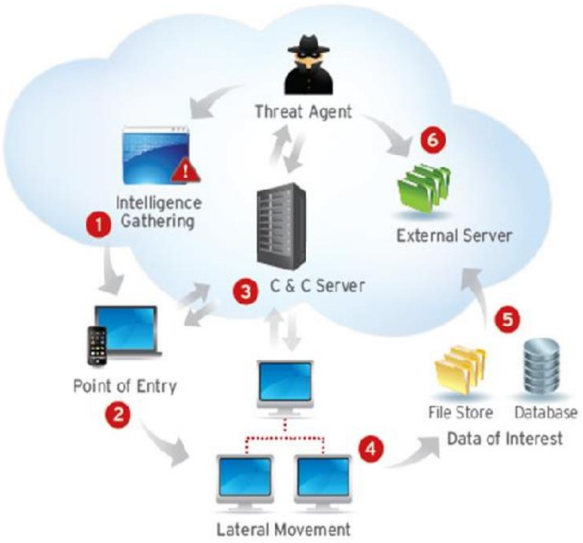

Fig: Typical steps of APT attack

The advanced persistent threats may be sponsored by state or organized crime groups to use advanced and latest methods including Spear Phishing, Social engineering techniques, anti-sandboxing, code rewriting etc., to gain information they can use to carry out criminal acts for financial gain.

APT groups achieve access to a company or organization by targeting devices via the internet, spear phishing emails or an application vulnerability with the aim of using malicious software in the target to leverage any access.

Then threat actors use their access obtained to further recon the organization network and start exploiting the malware they have installed to generate backdoor.

They use advanced password cracking methods to obtain high level administrative access to control more systems in the organization and to get access to different security areas of the organization.

Once the attackers have the access to sensitive and high valuable data of the organization, they use advanced methods to compress and encrypt that data which can be exfiltrated with ease.

The attackers after exfiltrating the sensitive data, they may repeat the same process for ages until they are detected which is easy for them to access the systems in the organization again at the same point.

Some of the Advanced Persistent threat examples:

1) APT41 - is a prolific cyber threat group that carries out Chinese state-sponsored espionage activity in addition to financially motivated activity potentially outside of state control.
2) APT40 - is a Chinese cyber espionage group that typically targets countries strategically important to the Belt and Road Initiative.
3) APT39 - The group's focus on the telecommunications and travel industries suggests intent to perform monitoring, tracking, or surveillance operations against specific individuals, collect proprietary or customer data.
4) APT28 – Russian government sponsored group which is a skilled team of developers and operators collecting intelligence on defense and geopolitical issues.
5) APT29 - APT29 is one of the most evolved and capable threat groups. It deploys new backdoors to fix its own bugs and add features. It monitors network defender activity to maintain control over systems.
6) APT1 - has systematically stolen hundreds of terabytes of data from at least 141 organizations and has demonstrated the capability and intent to steal from dozens of organizations simultaneously. The group focuses on compromising organizations across a broad range of industries in English-speaking countries.
7) APT18 – The Chinese group that targets Aerospace and Defense, Construction and Engineering, Education, Health and Biotechnology, High Tech, Telecommunications, Transportation sectors.

Advanced Persistent threats should be prevented, detected as early as possible to save the organizations from losing its valuable data and huge financial loss.

Detection of APT attacks is challenging because of its obfuscated nature. There are some indications, however, that organizations can pay attention to:

Unexpected traffic - from internal devices to other internal or external devices in the form of unusual data flows. This might be a sign that communication is taking place with a Command and Control (C2) server.

Suspicious logons - when account privileges are accessed outside hours of company. This may indicate that APTs are quickly spreading across the network, gathering sensitive and valuable data.

User and entity behavior analytics (UEBA) - is an essential tool for uncovering APTs. They are increasingly using artificial intelligence (AI), monitoring and analyzing how users interact with the IT systems of an organization and detecting anomalous behavior.

Recurring malware - particularly backdoor malware. This sort of infringement enables future exploitation of the APT threat actors. When mitigated malware continues to return and infiltrate the network, there is a backdoor.

Network Monitoring - Network monitoring may reveal suspicious activity signaling an APT.

Unexpected bundles of information - composed of gigabytes of information appearing at places where the information should not be present. This could show APT activity, particularly if the information is compressed into archive formats that would usually not be used by the organization.

Targeted Spear-phishing Emails - Targets specific individuals at businesses, and spear-phishers use private data about their targets to make their messages more trustworthy and credible. Any emails sent by unidentified individuals to high-level company managers are red flags.

While APTs are sophisticated, the organizations can take below measures to prevent against advanced persistent threats.

As a first layer of defense,

Install Software firewalls, hardware firewalls, and cloud firewalls - which can help to identify and block traffic to prevent the organization from advanced persistent threats.

Enable a Web Application Firewall - which is a useful tool to defeat APT attacks by inspecting HTTP traffic from web applications.

Install an Antivirus - that can detect and stop a wide variety of malware, trojans, and viruses that will be used by APT hackers to exploit your system.

Implement Intrusion prevention systems (IPS) - essential IT security service that monitors your network for any strange behavior or malicious code and alerts you if any is found.

Create a Sandboxing Environment - A sandbox is a safe, virtual environment that enables you to open and execute untrusted programs or codes without harming your operating system.

Install a VPN - Risks of remote access, such as an unsafe Wi-Fi hotspot, offer a simple chance for APT hackers to obtain original access to the network of your company.

Enable Email Protection – To get spam and malware protection for email applications.

To further prevent APTs, use the below as next layer of defense

Employee training - Many APTs begin with a fraudulent email that gives your system access. Deploy a training program that teaches staff what to look for, what to do, and who to notify if something suspect is detected. The best way to mitigate hazards is to stop an assault before it begins.

Penetration testing - It's a tried and tested way to unravel the safety deficiencies of an organization. Whether it was carried out internally with red teams (attackers) and blue teams (defenders) or with an external penetration test service. This training can be used to support the cyber-defense of an organization and to maintain IT safety teams on their toes. Set up a threat-hunting team and set up continuing vulnerability testing.

Ensure all Security patches are installed - APT hackers seek to exploit any weaknesses in your system, so it is vital to run updates on all cybersecurity programs. If you avoid or delay updates and patches, you leave your business vulnerable to attacks.

Improved security of most sensitive data - Consider using your most delicate data to take extra safety steps. If they don't need them, don't automatically assign administrator rights to personnel accounts. Limit data access and editing capacities to decrease the chance of accidental modifications.

APTs can be a business that is highly damaging. If you think your business is at danger, an experienced cybersecurity firm is the best way to mitigate these hazards. Look for one that provides both APT Intelligence Reporting and support for identifying and stopping threats.

Access control - APTs cannot damage what they can't reach. Access control enables IT departments use a variety of access policies and parameters to block attacks. If a device on a network fails an automatic security check, access will be blocked by a Network access control solution, preventing APT spread.

Administrator controls - only IT administrators and qualified personnel should be granted administrator access.

References: Fig- Typical steps of APT attack-www.researchgate.net