Advanced persistent threat (APT) refers to a broad term that is used to describe an attack campaign in which an attacker or group of attackers get unauthorized access to systems and networks over an extended period to mine highly sensitive data. The term was initially used in the military before it was adapted into the information security context. While APTs resemble other threats to some extent and are usually mixed up with the term targeted attacks due to the complex nature of both, APTs actually consist of complex stages and are more sophisticated in nature requiring deft knowledge and skills to execute (APT [Advanced Persistent Threat], n.d.).

Threats related to APTs are created by a group of developers who utilize in-house tools that aren’t usually found in the cybercriminal underground. Additionally, the attacks are carried out by nation-states making such attacks different from targeted attacks (attacks that have different targets and aren’t launched by nation-states). That being said, APT attacks also differ from web application attacks due to their significant complexity, long-lasting behavior, a large area of impact, and manual execution (What is an APT, n.d.).

Successful execution of APT involves three main stages: Infiltration, Expansion, and extraction.

* Infiltration: This stage involves infiltrating the target by using various attack surfaces such as web assets, network resources, or humans. The process is achieved by using malware, social engineering, or simultaneously executing a Distributed Denial of Service (DDoS) attack. Once initial access has been realized, attacks install a backdoor shell (malware) that grants access to resources.
* Expansion: During this stage, attackers broaden their access by moving across the network and compromising assets and users to gather critical business information or other sensitive data. The ultimate goal is to sabotage the victim by manipulating the data and selling the information to an unauthorized entity.
* Extraction: After collecting the data, the attacker finds a way to extract the information without being detected. To make this possible, the intruder weakness security controls or launches another attack such as a DDoS to shift the attention of the security team to the attack instead of the extraction. When the extraction process is complete, the attacker has already covered its traces, and the victim’s environment remains normal or not attacked (What is an APT, n.d.).

As a result, the consequences resulting from APT related attacks include:

* Intellectual property theft
* Compromised sensitive data
* Total assets and network takeovers and
* Sabotage of critical infrastructures ( power grids, nuclear reactors, or fuel pipelines).

Some examples of APTs include Stuxnet, which took down Iran’s nuclear program and Hydrag, a family of threats used in sophisticated attacks against high-profile networks, including the 2009 Operation Aurora campaign that targeted Google and other U.S. companies. Stuxnet targeted specific Siemens industrial control systems and CPUs to physically destroyed the centrifuges that enriched the uranium in computers. On the other hand, Hydraq used a zero-day exploit to install a malicious Trojan horse named Hydra to attack adobe systems, banks, defense contractors, security vendors, oil and gas companies, and other technology companies (Maloney, 2018).

Proper APT detection and protection require a multi-layered approach by network admins, security providers, and users. One way of detecting flaws and vulnerabilities in the layered approach involves conducting penetration tests. Penetration testing can simulate an actual APT attack by following the same procedures (from reconnaissance to infiltration and extraction) ethically to check for exploitable vulnerabilities, thereby providing insights to tighten security policies such as Web Application Firewall (WAF), modify or add security controls, train users, and patch systems. Hence uncovering possible exploits used by APTs such as Stuxnet and Hydrag can be possible. In fact, penetration testers can use custom APT such as Acarus (an APT used by the Tarlogic Ethical Hacking team) to test organizations’ infrastructural security controls.

References

APT [Advanced Persistent Threat]. (n.d.). Trend Micro. Retrieved from https://www.trendmicro.com/vinfo/us/security/definition/advanced-persistent-threat

Maloney, S. (2018). What is an advanced persistent threat (APT)? Cybereason Blogs. Retrieved from https://www.cybereason.com/blog/advanced-persistent-threat-apt

What is an APT? (n.d.). Impreva. Retrieved from https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/