HOW ADVANCED PERSISTENT THREATS WORK

By XM Cyber Team

There seem to be as many definitions of APT as there are actual APTs. The term describes a non-opportunistic, group-breaching organization in a strategic, long-term manner with clear objectives. They will not easily be deterred until they have achieved what they set out to do.

Actors behind APTs create a growing and changing risk to organizations' financial assets, intellectual property, and reputation by following a continuous process or kill chain:

1) Target specific organizations for a singular objective
2) Attempt to gain a foothold in the environment (common tactics include spear-phishing emails)
3) Use the compromised systems as access into the target network
4) Deploy additional tools that help fulfill the attack objective
5) Cover tracks to maintain access for future initiatives

THE CYBER KILL CHAIN

A kill chain is used to describe the various stages of a cyberattack as it pertains to network security. The actual model, the Cyber Kill Chain framework, was developed by Lockheed Martin and is used for identification and prevention of cyber intrusions.

The actual steps in a kill chain trace the typical stages of a cyberattack from early reconnaissance to completion. Analysts use the chain to detect and prevent advanced persistent threats.

According to Lockheed Martin's APT documentation, the seven steps of the Cyber Kill Chain include the following:

- Reconnaissance – Example: harvest email accounts
- Weaponization – Example: couple an exploit with a backdoor
- Delivery – Example: deliver bundle via email or Web
- Exploitation – Example: exploit a vulnerability to execute code
- Installation – Example: Install malware on the target
- Command and Control – Example: Command channel for remote manipulation
- Actions on Objectives – Example: Access for the intruder to accomplish the goal

MITRE ATT&ACK

Approaches for the detection of APTs are subject to considerable hype. It is common to hear about specific attack methods and how these techniques can evade the usual defenses employed by organizations. Yet the critical tools required to detect, investigate and respond to targeted attacks requires a holistic view of the attack lifecycle and a real-world understanding of the attacker's intent.

This is where the MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) framework really shines. MITRE ATT&CK is a model developed from years of actual observations of how adversary groups operate. Think of a law enforcement investigator carefully documenting the methods of operation of a criminal syndicate – the resulting profile is not only a historical document of past behavior, but a powerful tool to identify and predict how that syndicate will behave in the future. This is exactly what MITRE ATT&CK enables an enterprise to do with adversary groups that have their firm in the crosshairs.

One key aspect of MITRE ATT&CK is that any specific technique detected also needs to be understood in the content of the larger attack pattern and environment in which the detection occurred. Analysts need tools that deliver detections with contextual details that help the analyst prioritize their investigations.

CHALLENGES IN ADVANCED PERSISTENT THREAT DEFENSE

As you might imagine, defending against APTs can be quite challenging. By design, they are extremely hard to detect. And, their dormant, persistent nature makes them difficult to stop once they've taken root. You might think you've quarantined it, but it's already replicated and hidden elsewhere.

They are even able to elude AI-driven anomaly detection. Indeed, APTs may mimic the behaviors of real users and appliances, so they don't trigger alerts. To defend against an APT, you need countermeasures that are also advanced and persistent. It won't work to use legacy security tools that are episodic and reactive. You must go hunting the problem. Then, once you start, you cannot stop hunting because hackers create a continuous threat.

COUNTERMEASURES FOR APT CYBER THREAT

APTs put intolerable pressure on enterprise cybersecurity countermeasures. Generally reactive in nature, today's standard cybersecurity controls are overly reliant on detecting and responding to immediate incidents. This approach may be suitable for some attacks, but it does not work well with slow-moving, stealthy APTs. For better defense, enterprises are starting to turn to Breach and Attack Simulation (BAS) solutions, which test security on an automated and continual basis.

ABOUT XM CYBER

XM Cyber was founded by security executives from the elite Israeli intelligence sector.

XM Cyber's core team is comprised of highly skilled and experienced veterans from the Israeli Intelligence with expertise in both offensive and defensive cyber security.

XM Cyber has developed more than 15 patented technologies based on a proprietary set of algorithms that enable the continuous and automatic simulation of a hacker's techniques and methods.

XM CYBER TEAM

The XM Cyber team consists of the best cyber security specialists in the world. Their thought leadership helps inform and educate customers globally via webinars, videos, articles, books and industry presentations. Join us online at xmcyber.com for more in-depth analysis and recommendations on cyber security best practices.