Advanced Persistent Threats (APT)

What's an APT? A Brief Definition

Advanced Persistent Threats (APTs) require a high degree of stealthiness over a prolonged duration of operation in order to be successful. The attack objectives therefore typically extend beyond immediate financial gain, and compromised systems continue to be of service even after key systems have been breached and initial goals reached.

Definitions of precisely what an APT is can vary widely, but can best be summarized by their named requirements:

Advanced – Organizations behind the threat utilize the full spectrum of computer intrusion technologies and techniques. While individual components of the attack may not be classed as particularly "advanced" (e.g. malware components generated from commonly available DIY construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They combine multiple attack methodologies and tools in order to reach and compromise their target.

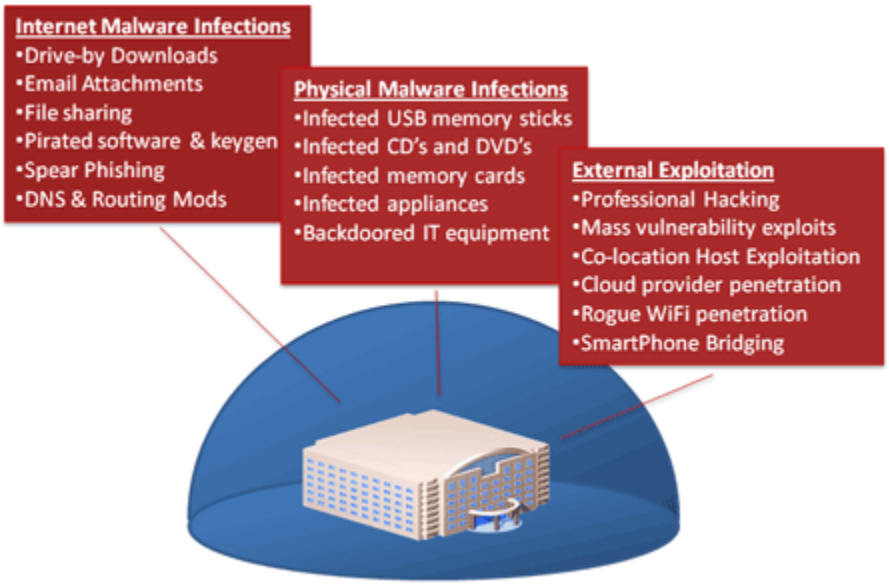
Persistent – Organizations behind the threat give priority to a specific task, rather than opportunistically seeking immediate financial gain. This distinction implies that the attackers are guided by external entities. The attack is conducted through continuous monitoring and interaction in order to achieve the defined objectives. It does not mean a barrage of constant attacks and malware updates. In fact, a "low-and-slow" approach is usually more successful.

Threat – means that there is a level of coordinated human involvement in the attack, rather than a mindless and automated piece of code. The Organizations behind the threat have a specific objective and are skilled, motivated, organized and well funded.

How Advanced Persistent Threats Breach Enterprises:

APTs breach enterprises through a wide variety of vectors, even in the presence of properly designed and maintained defense-in-depth strategies:

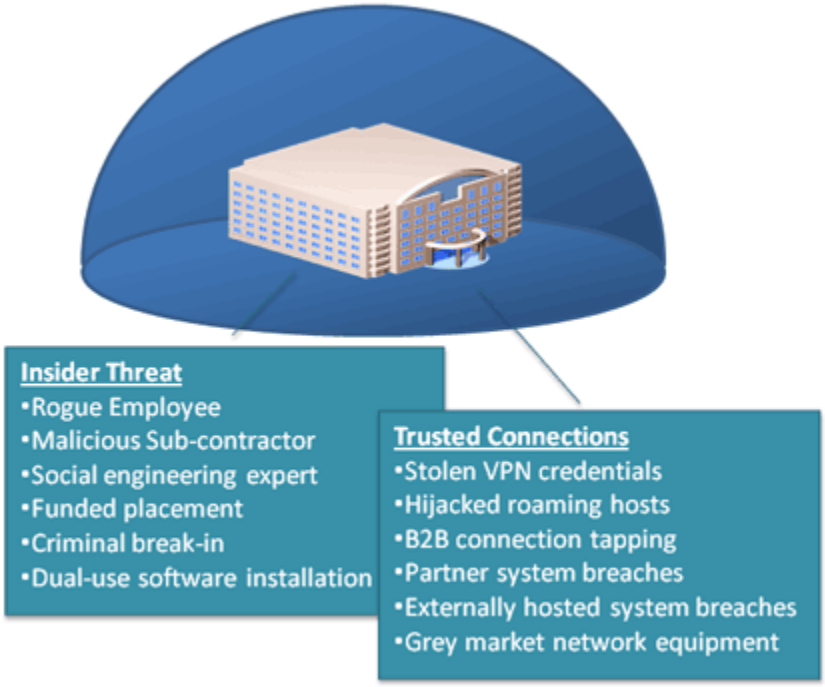
- Internet-based malware infection
- Physical malware infection
- External exploitation



Well funded APT adversaries do not necessarily need to breach perimeter security controls from an external perspective. They can, and often do, leverage "insider threat" and "trusted connection" vectors to access and compromise targeted systems. Well-funded APT adversaries do not necessarily need to breach perimeter security controls from an external perspective. They can, and often do, leverage "insider threat" and "trusted connection" vectors to access and compromise targeted systems.

Abuse and compromise of "trusted connections" is a key ingredient for many APTs. While the targeted organization may employ sophisticated technologies in order to prevent infection and compromise of their digital systems,

operators often tunnel in to an organization using the hijacked credentials of employees or business partners, or via less-secured remote offices. As such, almost any organization or remote site may fall victim to an APT and be utilized as a soft entry or information harvesting point.



A key requirement for APTs (as opposed to an “every day” botnet) is to remain invisible for as long as possible. As such, the operators of APT technologies tend to focus on “low and slow” attacks – stealthily moving from one compromised host to the next, without generating regular or predictable network traffic – to hunt for their specific data or system objectives. Tremendous effort is invested to ensure that malicious actions cannot be observed by legitimate operators of the systems.

Malware is a key ingredient in successful APT operations. Modern “off-the-shelf” and commercial malware includes all of the features and functionality necessary to infect digital systems, hide from host-based detection systems, navigate networks, capture and extricate key data, provide video surveillance, along with silent and covert channels for remote control. If needed, APT operators can and will use custom developed malware tools to achieve specific objectives and harvest information from non-standard systems

At the very heart of every APT lies remote control functionality. Operators rely upon this capability in order to navigate to specific hosts within target organizations, exploit and manipulate local systems, and gain continuous access to critical information.

If an APT cannot connect with its operators, then it cannot transmit any intelligence it may have captured. In effect, it has been neutered. This characteristic makes APTs appear as a sub-category of botnets.

While APT malware can remain stealthy at the host level, the network activity associated with remote control is more easily identified. As such, APT’s are most effectively identified, contained and disrupted at the network level.