

Advanced Persistent Threats

Fight large-scale threats with unified solutions and advanced intelligence from McAfee



Advanced persistent threats (APTs) have many definitions. In most cases, it's an over-used and abused marketing term adopted by point solution security vendors to talk about their ability to stop "bad things." The term most generally defines an adversary with formidable means, organization, and motivation. While more encompassing, it is often associated with espionage, and, as such, the concept predates the digital era and can be traced back to the earliest documentation of intelligence gathering recorded by military strategists such as Sun-Tzu and Chanakya.

Talking about APTs has become increasingly popular over the past year. This is in part because of a series of cyberattacks dubbed Operation Aurora. These attacks started in mid-2009. Google, Northrop Grumman, Dow Chemical, and around 30 other companies were targeted, and it has been speculated that these attacks originated in China. Operation Aurora was considered an APT because the attacks were sophisticated, targeted, stealthy, and designed for long-term manipulation of the targets. Over the last decade, there have been several other attacks thought to be from China that could fall into the APT category, including:

- *Titan Rain*—A series of attacks in 2003 that extracted information equivalent in size to the Library of Congress from Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, NASA, and several other government organizations
- *F-35 Joint Strike Fighter*—In 2009, The Wall Street Journal reported that the Pentagon's \$300 billion project had terabytes of data stolen

Some organizations may feel that they are not "important" enough to worry about APTs. Organizations need to consider their industry, geographical location, partners, and suppliers. Situational awareness around interactions on a global market level and the interest other organizations might have in organizational assets is critical to determining what may be worth attacking, and, as such, worth protecting. Some organizations may be targeted specifically because they have lax security and because they also have partnerships that yield higher value targets. This makes them a leapfrog candidate that attackers can use to conduct reconnaissance and information extrusion from the partners. Other organizations simply have valuable information and or sensitive hard assets, so they are an obvious target.

Characteristics of Advanced Persistent Threats

The characteristics of APT can best be analyzed by exploring four critical factors, including actors, motives, targets, and goals.

Actors

There are several actors that have been associated with APTs ranging from terrorists, activists, and organized crime groups to unscrupulous competitors, ex-employees, and malicious insiders. Perhaps the most common are nation-states, that is, a state or country with defined borders and territory. Since APTs generally require more resources than other cyberattacks, look for the groups with the greatest resources: military and intelligence organizations. When the aggressor is a nation-state, the concept

of APT often merges with common definitions around information warfare. According to the FBI, more than 100 countries now have information warfare capabilities. But when information warfare is conducted by nation-states, non-state entities can and indeed have participated, creating a force multiplier. This is simply due to the fact that the Internet and computing resources allow patriots and sympathizers who don't work for a government to take advantage of remaining anonymous, leveraging inexpensive technology with global range, and taking advantage of attack vehicles such as scripts and bots. Some of these attack vehicles were designed by nation-states to aid in conducting espionage, spreading propaganda, or launching attacks such as denial-of-service (DoS) attacks. Some examples of these are:

- Vladimir Putin, Prime Minister of Russia, commands a youth group call the Nashi. It has been claimed that Russian operatives will occasionally post instructions for the Nashi on downloading and launching DoS attacks against predefined targets.
- In May 2007, three weeks of cyberattacks were launched on Estonia following the removal of a bronze soldier. More than 80,000 IP addresses were identified as sources of attack. Many of these IPs were traced back to the Russian mafia, as well as Russian sympathizers in Latvia, Ukraine, and the U.S.
- In April 2008, CNN was reporting on Tibet. More than 5,000 Chinese forums began recruiting patriots to allow their computers to be infected with the botnet AntiCNN.exe to block the coverage in China. CNN responded by blocking all access to their systems from Chinese sources, thus accomplishing the attackers' goal directly through the DoS attacks and because CNN responded by blocking Chinese access.

Motives

There are a broad range of motivations for these actors, but like most cyberattacks, they are rooted primarily in economics. However, ideology shouldn't be dismissed, as outlined in earlier examples. Consider an APT of insiders conducting espionage. A paper entitled *Espionage by the Numbers* by Richard J. Heuer, Jr. of the Defense Personnel Security Research Center analyzes decades of espionage information and shares very telling statistics regarding motivations:

- Primarily motivated by money: 69%
- Only motivated by money: 56%
- Disgruntlement or revenge: 27%
- Ideology: 22%
- Desire to please: 17%
- Excitement: 12%
- Coerced: 05%
- Importance: 04%

The desire for money—either driven by need or greed—remains by far the strongest motivator.

Targets

Given the previous actors and their motives, the targets are really quite intuitive. As discussed earlier with respect to Titan Rain and Operation Aurora, the actors are most commonly, but not always, targeting large corporations, government organizations, defense contractors, academic intuitions, the media, and critical infrastructure. Attacking these organizations often requires a significant investment and, like any investment, is done in hopes of a reward—either economic, political, or both. Consider an APT that is targeting critical infrastructures, such as electric power, nuclear, water, or chemical facilities.

A worm named Stuxnet was discovered in the third quarter of 2010 and was based on an earlier version developed in 2009. It is the first purpose-built worm designed to attack programmable logic controllers (PLC), industrial control systems that help run critical infrastructure environments. PLCs are not an ideal target for an adversary to use for espionage or extortion; there are better targets for that. As such, it can be hypothesized that Stuxnet was designed purely to attack PLCs and cause damage to the infrastructure they operate and, ultimately, to the people and organizations that depend on that infrastructure.

Stuxnet is clearly an example of a stealthy worm developed by an adversary that spent a great deal of time and money on research and development. While the origins are still unknown, many experts feel that it was likely developed by a nation-state with nefarious intent driven by political rather than economic motivations.

Goals

Actors, motives, and targets are disparate, and, as such, so are their ultimate goals. However some operational goals seem to be constant:

- Using stealth during intrusion to avoid detection
- Creating backdoors to allow greater access, especially if other access points have been discovered and patched
- Initiating the primary mission:
 - » Stealing sensitive data
 - » Monitoring communications
 - » Disrupting operations
- Leaving undetected

Why Mitigating Advanced Persistent Threats Is Difficult

Many APTs are designed specifically for stealth operations and can move from compromised system to system without generating the predictable network traffic often seen when malware propagates. APT attacks are often developed to evade traditional anti-malware solutions and intrusion prevention systems (IPS) and are uniquely compiled for a specific organization or industry, as was the case with AntiCNN.exe and Stuxnet.

Most point security solutions operate in a silo and are designed to address a particular crime of opportunity. This disconnected approach to security rarely works with opportunistic attacks and simply won't work with targeted ones. It's analogous to trying to find the malicious needle in the haystack using a microscope. Solutions in silos don't enrich each other with relevant data and introduce greater complexity to analysis and remediation, giving the advantage to the perpetrators of the APT.

What Are the Impacts of Advanced Persistent Threats?

Many a Hollywood movie plot is conceived about the implications of large-scale attacks, cyber or otherwise. The theft of intellectual property tops the list, as previously discussed in the case of Titan Rain and the F-35 Joint Strike Fighter. There have been instances where organizations have lost millions and even billions in research information. In some cases, organizations have even gone bankrupt because of their inability to cost effectively compete with malicious competitors that have stolen their intellectual property (IP).

This was the case in the 1990s with Ellery Systems in Boulder, Colorado when an employee sent sensitive information to a competitor in China—Beijing Machinery. This led to Ellery going out of business and was, in part, responsible for the creation of the 1996 Economic Espionage Act. Another example is DuPont, where an employee, Gary Min, stole \$400 million in IP to bring with him to an Asian competitor, Victrex, in 2005. A few years later, another DuPont employee stole IP relative to a new paper-thin monitor and gave it to his alma mater, Peking University in Beijing. Unfortunately, these stories are all too common. Regardless of who the perpetrator may be—a malicious insider, a plant, mole, or external attacker—sensitive data has value to cybercriminals and is being targeted aggressively.

These types of attacks can impact revenue, brand, and shareholder faith and can lead to class-action lawsuits and regulatory penalties. But the real nightmare scenarios are attacks against critical infrastructures, such as the electric grid.

Consider an attack with a goal of invading another country using traditional kinetic warfare, for example bombs and bullets. By just attacking the electric grid by way of a cyberattack, there is a massive trickledown effect:

- Electric power goes off
- Because electric systems power the safety systems for other power-producing plants like nuclear plants, they need to shut down too
- After a few days, supply chains aren't being replenished, and gas stations, ATMs, and grocery stores are depleted
- At the same time, looting and rioting begins
- Hospitals and emergency services are not be able to keep up
- Military forces are called on to keep the peace among the populace

This type of APT attack on the electric grid could result in weakening, distracting, and disorienting social cohesion. The disruption in infrastructure, logistics, and supply chains can cause low political will and is fueled by chaos, which opens up an opportunity for a kinetic attack. While this nightmare scenario seems steeped in fiction more than in fact, there have already been instances of the convergence of kinetic and non-kinetic warfare, such as the Russian attack on Georgia in August 2008. During this attack, information warfare was used to hinder the operations of key communication networks, such as radio stations, while tanks opened fire.

What McAfee Can Do

Mitigating APTs is part of our DNA. For decades McAfee has been helping organizations mitigate risk. It is precisely these complex security problems where McAfee, offering unified and cohesive solutions across mobile devices, system assets, networks, and data, excels at protecting some of the most sensitive organizations in the world for years. There is no silver bullet for APTs because it's more than firewall and IPS, more than anti-malware, and more than data loss prevention. This is truly a case where whole is greater than the sum of its parts.

No other organization in the world is better positioned to address ATPs than McAfee. Consider Operation Aurora. Following the detection of the attacks that would later be called Operation Aurora, McAfee quickly added anti-virus protection for customers. Later, Google and Adobe announced the attacks publicly. McAfee then identified the zero-day vulnerability in Microsoft Internet Explorer that was used in these attacks and named it "Operation Aurora," while integrating countermeasures into the McAfee Network Security Platform to further secure its customer base. The speed and agility of McAfee were second to none in the identification, analysis, and countermeasures for Operation Aurora.

By merging traditionally disparate product solution such as network controls and anti-virus technologies within a unified solution, not only are the products easier to manage, but attacks are detected and investigated more efficiently and effectively and incident response is more rapid. The McAfee Global Threat Intelligence™ network offers a distinct advantage by providing advanced reconnaissance into attacker behaviors and techniques to prevent attacks from penetrating sensitive assets before the attacker gains a foothold.

In some situations, organizations may have already fallen victim to an attack, and they don't know where to turn. McAfee offers the broadest set of security expertise in the world, specializing in aiding organizations that have suffered attacks. The collective intelligence that is leveraged in the McAfee products for attacker behavior and technique identification can be used by McAfee services teams to better understand details about an organization's particular attackers.

Let's consider some APT use cases that illustrate core capabilities delivered by McAfee.

Theft

Scenario: A competitor is interested in stealing intellectual property from a biotech company. Instead of hacking in from the outside and risking detection, the competitor recruits a trusted employee who has legitimate access to the desired material.

Attack: The malicious insider wants to use his legitimate access privileges to download structured data from databases and unstructured data from file servers. He will attempt to amass as much sensitive data as possible onto his workstation and then copy it to removable media to physically remove it from his employer's premises.

Mitigation: McAfee has the ability to monitor how users interact with data, and that includes employees, outsiders, privileged users, and others. By using a combination of host-based and network-based data loss prevention in conjunction with advanced correlation, anomaly detection, and pattern discovery capabilities, even legitimate access that deviates from the norm—such as users downloading excessive amounts of information in a short time period, accessing information at unusual times, or accessing high-value information of multiple types from too many different sources—can raise flags. This combination of machine-based analytics and human analysis and intuition can help mitigate sensitive data breaches like this even when they appear to be wrapped in the cloak of acceptable activity.

Surveillance

Scenario: A nation-state is attempting to glean information related to troop movements of a country with which it is currently having disputes.

Attack: The attackers are armed with a substantial botnet infrastructure that spans the globe and malware specially designed to log keystrokes, monitor network traffic, and take screen shots while periodically encrypting and sending the information to a centralized collection site. The attackers want to use the botnets for spear phishing (targeting specific military personnel) and trick them into opening up an "image file" that is really an executable that will ultimately be downloaded and install the entirety of the malware.

Mitigation: McAfee addresses this type of attack on multiple levels. McAfee Global Threat Intelligence uses an elaborate combination of sensors and researchers across the world to constantly track malicious IPs, domains, geographies, activities, and patterns, and generate real-time information about threats, such as data related to botnets. This intelligence is automatically refreshed within McAfee products to prevent those malicious sources from ever being able to enter the network environment through any mechanism, including phishing emails and instant messaging. Additionally, the McAfee firewall can detect nefarious attachments that are impersonating benign files, thus shutting down the attacker's attempts to use social engineering to trick users. This multipronged approach provides intelligent defense in depth.

Sabotage

Scenario: A terrorist organization is targeting the electric power grid of a country with contrary political beliefs. The terrorists' goal is to cause long-term blackouts in major cities.

Attack: The terrorist group has created purpose-built malware designed to target and take over PLCs, which are responsible for managing critical areas within the electric power grid, by exploiting a zero-day vulnerability.

Mitigation: McAfee has solutions specifically designed for specialized systems such as PLCs, point-of-sale systems, ATMs, multifunction printers, and other fixed-function servers. By using dynamic whitelisting, McAfee will not allow the installation or execution of any programs that have not been explicitly allowed. This is particularly useful for PLCs and other industrial control systems found in critical infrastructure because dynamic whitelisting from McAfee is not scan based, doesn't require updates or even network access, doesn't depend on blacklisting (signatures), and can be centrally managed. This combination

of capabilities is vital, as traditional anti-malware solutions will be too large, too process- and memory-intensive, and require frequent updates. As such, the terrorist organization's malware won't be allowed to run or even be installed on the PLCs, thus preventing the attack.

Regardless of whether a single attack vector or multiple attack vectors are involved, McAfee connects the security dots, enriches them with threat intelligence, and provides the countermeasures needed to mitigate risk rapidly and definitively.

The unique combination of McAfee products, services, partners, and threat research manifests in a cohesive, strategic solution for mitigating APTs, regardless of the source—malicious insiders, unscrupulous competitors, or nation-states. It doesn't matter if the motives are economic or political, the targets are government organizations or commercial businesses, or if the goals are to cause destruction or steal information. Organizations using McAfee solutions will be able to reduce risk, increase operational efficiencies, and achieve heightened ROI for their security investment—even in the face of APTs.

For more information on the McAfee solutions for advanced persistent threats (APTs), please visit: www.mcafee.com.

