Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 9, Issue 2

Behavior Analysis for Discovery and Countering Advanced Persistent Threats

By Antonio Nucci

Advanced persistent threats (APTs) continue to be a major concern for network operators. In fact, last November, Enterprise Strategies Group released a study that indicated 59 percent of enterprises with at least 1,000 employees had been hit by an APT; 72 percent believe they'll be hit again. They are indeed insidious, and spark fear in network operators charged with protecting our most critical networks. This is because they are designed to spy on their target for long periods of time, blending in with a network's day-to-day traffic and appearing unremarkable, therefore being dismissed by security solutions and network operators alike as innocuous. Given this, as well as the fact that the integrity of our critical networks hangs in the balance, the sense of urgency to understand APTs and learn how best to mitigate them is palpable.

APTs 101: A Primer

Abraham Lincoln once said, "I don't like that man. I must get to know him better." Such is the case with APTs, for while mitigating them is of great importance, understanding them is equally critical if we are to stay one step ahead of cyber criminals. With that in mind, this section is dedicated to a brief education on the stages and nature of an APT attack.

A single piece of malware often has multiple characteristics. Its digital signatures can morph to evade detection. It can develop decoys to make it appear as if an attack has been thwarted. APT attacks are sometimes waged by teams of hackers who try to infiltrate different levels of the infrastructure (i.e. network level or host level). They use "designer" code (malware) to circumvent most common defenses, and focus their tools and techniques on a specific target. In essence, the shotgun attacks of the past have migrated to ones that are purposeful and targeted to specific people, companies and even servers.

Understanding the stages of an APT enables an organization to address, thwart and potentially mitigate the attack. The first objective of an APT is to determine a target. The end target could be a person, a company, a government organization, or a specific server or application. Attackers will often target specific people (could be anyone, from administrative assistants to executives) to gain entry to an organization's network. Attackers will use public search or other methods to obtain their targets' email addresses or instant messaging handles, thereby building a profile on their targets. Next, a "seed" is planted, infecting machines and networks. Common channels are emails from eBay, PayPal or a bank, indicating a purchase, a problem with a purchase, or just a verification of identity. A bot is then exploited, and maintains tenacity and persistence. This is the crafty part of the APT as the attacker uses a variety of methods, including morphing their malware, to prevent detection. They then can establish additional footholds in the network and on the endpoints.

Behavior Analysis: Sniffing Out Attacks in Disguise

Many operators rely on traditional defenses like firewalls and intrusion detection system/intrusion prevention (IDS/IPS) systems to protect critical

The threats are no longer static and constrained.

networks, and, before we go any further, it's worth noting that these solutions are more than adequate for detecting known threats. This is because when operators know what the network signature of a given piece of malware looks like, it's reasonably straightforward to find.

But cyber criminals are crafty. They evaluate their defenders' responses and defenses and escalate their attack techniques accordingly. The threats are no longer static and constrained. This is why relying on traditional defenses to protect data from open ports or operating system vulnerabilities is no longer enough. Rather, obtaining real and actionable information is critical: being able to detect continual attempts to infiltrate a network, find infected hosts and enable security operations to execute forensics.

Given these requirements, behavioral analysis emerges as the best approach. Rather than looking for known threats (like traditional systems do), behavior analysis looks at all the traffic, tracking seemingly innocuous patterns (that may not necessarily be a red flag) in a network and pinpointing an APT. For example, tracking the average size of inbound and outbound emails will aid in discovering if an email is potentially infected, thus advising the recipient to not open it. Accuracy is improved by looking at a large number of sessions over a long period of time. By tracking and trending common L7 elements, the anomalies essentially “jump” out. These behavior analysis tactics, along with being familiar with your network and its patterns, will mean a higher chance at uncovering an APT.

A Group Effort

While behavioral analysis is a good start, there is no single solution on its own that is adequate to protect against APTs. Forensic analysis vendors and security and event management (SEM) vendors can provide part of the solution, but there is no one company that can provide a singular technical solution. Moreover, technology alone is inadequate. Computer security, systems integrator and consulting firms provide services, products and education to commercial and federal clients, and can provide a variety of technologies for a defense-in depth solution. Consulting companies combine a consultant’s knowledge of the APT with their unique technology, or that of their partner’s, to provide clients with another component of the solution. Companies that do “whitelisting” can be part of the holistic solution as well. Whitelisting can enable authorized access for specific software, applications and services. Whitelisting companies defend the endpoints against APTs by simply preventing the introduction of any unauthorized code to endpoints. Without the ability to deposit malware, the criminals lack the visibility, persistence and control they need to compromise their targets and achieve their objectives.

As threats evolve, the operator must be able to fully utilize new ways of detecting and combating these newer threats. The key is turning whatever information is gathered into actionable intelligence. While technology can help here, a more comprehensive solution must also address the need for better processes and training of our cyber warriors.

Over the past several years, there has been much discussion about situational awareness — the ability to understand what is happening on a network, from the traffic patterns to the context of changes in those traffic patterns. Indeed situational awareness is hailed as the foundation of network visibility, which is required to identify and combat any threat. Thus, by leveraging behavior analysis--along with partnerships and education--operators can attain situational awareness, and in turn, stop APTs in their tracks.

As threats evolve, the operator must be able to fully utilize new ways of detecting and combating these newer threats.