ESG
Enterprise Strategy Group | Getting to the bigger truth.™

White
Paper

Understanding and Addressing APTs

By Jon Oltsik, Senior Principal Analyst

September 2012

This ESG White Paper was commissioned by Trend Micro and is distributed under license from ESG.

Contents

Executive Summary

Three years ago, few people outside of the U.S. Department of Defense (DoD) or other military/intelligence organizations had heard of Advanced Persistent Threats (APTs). Now these kinds of targeted cyber attacks have become routine with discussion extending across the technology, business, and mainstream media.

Just what is an APT? Are they as big of a menace as the media portrays? If so, what are enterprise organizations doing about them? This white paper concludes:

- **APTs are unique and extremely dangerous.** The vast majority of security professionals believe that APTs are more than just hype. Furthermore, most large organizations are certain or believe it is likely that they have been the target of an APT. Little wonder then why 93% of security professionals are “very concerned” or “concerned” with the potential impact APTs could have on national interests.
- **Existing security controls are no match for APTs.** As with all security best practices, defense-in-depth is an important component for APT protection. The problem, however, is that APTs are designed to exploit cracks between layers of security technologies. APTs represent a new type of threat that demands solutions designed for detecting, blocking, analyzing, and monitoring them.
- **Large organizations need APT security solutions.** CISOs should certainly improve security processes, gain a better understanding of network activity, and get the most out of their existing security infrastructure. To address APTs however, they should consider specific network-based security tools that detect/prevent APT-based malware, and network communications, provide in-depth analytics capabilities, integrate with cloud-based security intelligence services, and improve the effectiveness of the existing security technology infrastructure.

An Overview of APTs

The term Advanced Persistent Threat (APT) was first coined by cybersecurity analysts at the United States Air Force in 2006. This idiom was then used to characterize specific types of threats in subsequent non-classified communications between military and civilian cybersecurity experts.

Typically, APTs are defined by parsing the acronym as follows:

- **Advanced.** APTs emanate from adversaries with strong technical skills in computer hardware, software, and networking. These adversaries are capable of developing and launching custom exploits as part of targeted attacks.
- **Persistent.** In a typical APT, an adversary invests time and resources in order to successfully penetrate a particular organization and exfiltrate some type of highly valuable data. These cyber adversaries are persistent in that they are willing to launch multiple exploits over multiple vectors until they achieve their nefarious goals.
- **Threat.** In information security terms, a threat is some type of danger that has the potential to exploit vulnerabilities, cause a security breach, and lead to measurable harm to the IT assets of an organization.

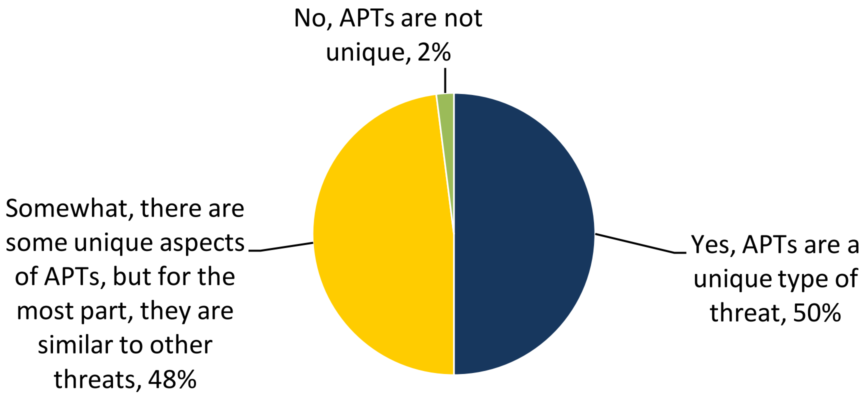
From 2006 through 2009, APT knowledge was really limited to military and intelligence services throughout the world as attacks were really focused on these sectors. That all changed in December 2009 with the Google Aurora attack. According to Google, this attack originated in China, targeted Google and several other large American companies (Adobe Systems, Juniper Networks, Rackspace, etc.), and resulted in the theft of Google Intellectual Property (IP). This single event transformed the term “APT” from an esoteric military acronym, to a topic worthy of mainstream media outlets. Since Operation Aurora, several other commercial enterprises including Morgan Stanley, RSA Security, and the World Bank have suffered APT attacks of their own.

Enterprise Organizations React to APTs

APTs share many characteristics with traditional "low and slow" hacking techniques intended to gradually compromise a network node over time, thus remaining invisible to intrusion detection and security monitoring systems. This begs the question: Are APTs really unique or nothing more than a marketing term used to describe well established attack methods? ESG posed this very question to 244 security professionals working at enterprise organizations (i.e., more than 1,000 employees) in a recent research survey. In spite of APT similarities with previous types of hacking tactics, 98% of security professionals believe that the sophistication, perseverance, and potential damage associated with APTs makes them "unique" or "somewhat unique" (see Figure 1).[1]

Figure 1. Security Professionals Believe that APTs Represent a Unique Type of Threat

Do you believe that sophisticated cyber attacks that have been described as APTs (e.g., Stuxnet, Aurora, Zeus, etc.) present a unique type of threat compared to other security threats? (Percent of respondents, N=244)

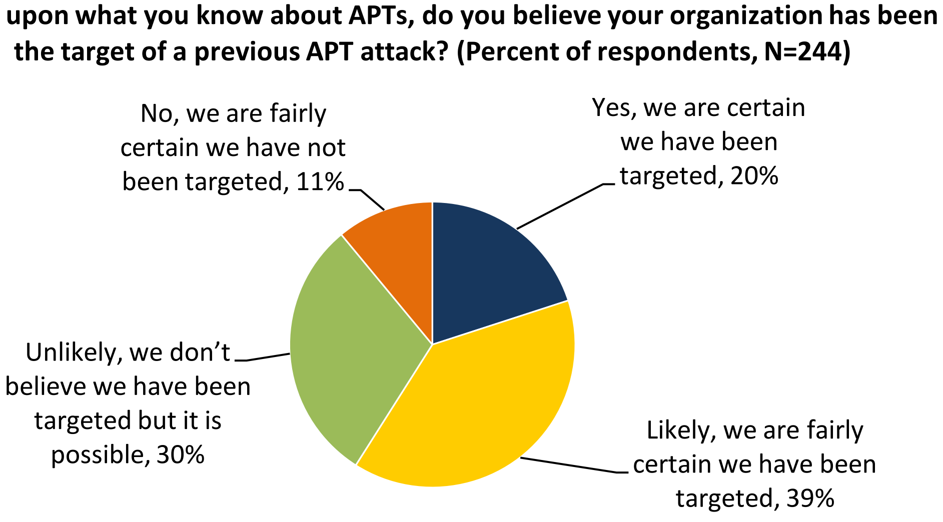


Source: Enterprise Strategy Group, 2011.

Aside from these visible attacks, APTs may be far more pervasive than most people believe. ESG research indicates that 59% of enterprise security professionals believe that it is "highly likely" or "somewhat likely" that their organization has been the target of an APT (see Figure 2). Alarmingly, 30% of enterprise organizations, including some that are amongst the most secure, believe they remain vulnerable to future APT attacks.

[1] Source: ESG Research Report, U.S. Advanced Persistent Threat Analysis, November 2011. All other ESG research references and charts in this white paper come from this report.

Figure 2. Belief that Organization Has Been Targeted by APTs



Source: Enterprise Strategy Group, 2011.

A high-ranking FBI official was recently quoted as saying that the "cyber threat can be an existential threat — meaning it can challenge our country's very existence, or significantly alter our nation's potential." When it comes to APTs, the security professionals surveyed by ESG completely agree—93% are "extremely concerned" or "concerned" about the impact that APTs could have on national interests, such as the domestic economy or national security.

APTs Circumvent Traditional Security Safeguards

The large organizations surveyed by ESG are responsible and diligent with information security practices for the most part. Given this, why do so many APT attacks find a way to circumvent millions of dollars of deployed security monitoring tools and intrusion detection/prevention technologies? APTs are often successful because:

- **Attacks start with convincing social engineering tactics.** To penetrate a specific organization, cyber adversaries gather intelligence on a few key employees by conducting web-based research and using social networking sites like Facebook, LinkedIn, and Twitter. Adversaries use this information to personalize their social engineering attacks in the hopes of establishing trust with a victim so they will download malicious code, open an attachment, or double click on a malicious link without questioning the source.
- **Endpoint security tools are not used effectively.** Nearly every enterprise endpoint system is instrumented with security software, but many aren't configured for maximum security protection. In some cases, the IT operations team retains historical biases that security protection will adversely impact endpoint performance which is no longer true. Other firms don't have the time or resources to learn the capabilities of modern endpoint security tools and use them most effectively. Finally, some organizations consider endpoint security a compliance "check box" and simply install the software to satisfy regulatory compliance mandates and IT auditors.
- **APTs exploit gaps between multiple security defenses.** APTs are designed to take advantage of the limitations of "islands of security" within IT. For example, many large organizations use separate tools for endpoint security, e-mail security, and web security with no overall policy management or oversight across all of them. APTs utilize these security enforcement and monitoring openings to squeeze their way into organizations.
- **APTs can look like normal network behavior to monitoring tools.** Once an initial endpoint is infected, APTs conduct multiple types of activities within the network. These include compromising additional systems, harvesting user/administrator credentials, locating/copying sensitive data, and finally transferring this data

to web-based servers. APT creators hide these activities within typical day-to-day communications and network activities. Most monitoring tools see nothing out of the ordinary.

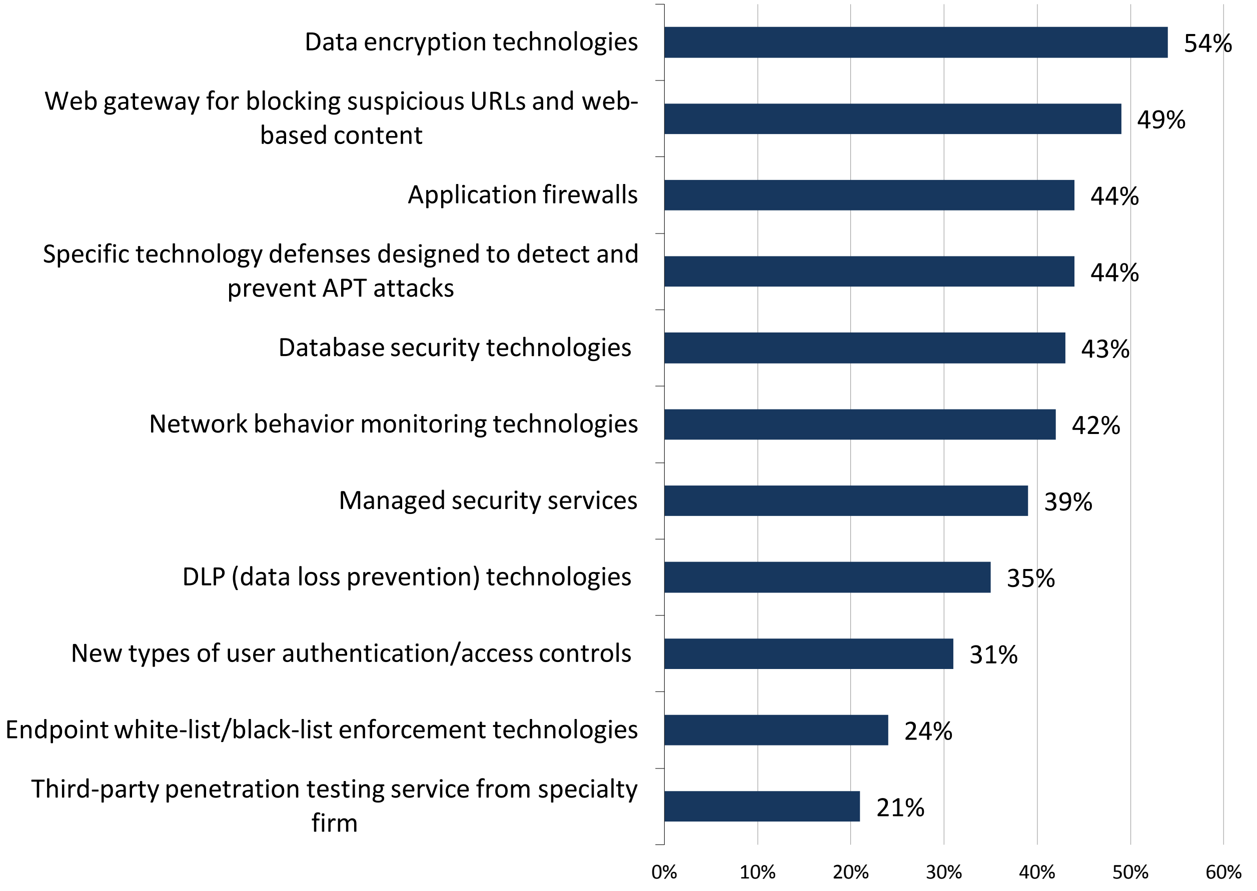
Enterprises Are Reacting to APTs

Unlike viruses, worms, and Trojans of the past, APTs and other sophisticated types of cyber attacks have finally garnered attention—all the way up to the corporate boardroom. According to ESG research, 47% of large organizations indicate that the recent series of APTs has caused their executive management to take new actions like increasing information security budgets, launching executive communications programs to alert employees to APT risks, and scheduling more frequent meetings with CISOs and the IT security team.

In addition to executive activity, ESG research indicates that nearly 40% of large organizations have already invested in new security technologies as a direct result of APTs. Which technologies? Data encryption technologies, web gateways, and application firewalls all top a long list of new investments (see Figure 3).

Figure 3. Technology Solutions Purchased in Response to APTs

Which of the following security technology products/solutions has your organization purchased in response to APTs? (Percent of respondents, N=95, multiple responses accepted)



Source: Enterprise Strategy Group, 2011.

Large Organizations Need APT Countermeasures

CISOs and corporate executives certainly recognize the dangers associated with APTs and are shoring up their defenses in response. Unfortunately, this action alone is not enough. In truth, APTs are designed to thwart a defense-in-depth security architecture as described above. Hardening existing security defenses, adding tactical security layers, or improving security processes may lower overall risk but this won't be enough to deal with the sophistication, and perseverance of APTs and similar types of targeted attacks.

To address APTs, large organizations need new security countermeasures specifically designed to address the unique tactics employed by APTs. APT security technologies should:

- **Detect the subtleties of APTs on the network.** APTs operate through a combination of malware propagation, Command-and-Control (C&C) communications, software downloads, and ultimately data exfiltration. To address this amalgamation of tactics, APT security technologies must be deployed on corporate networks for examining all ingress/egress traffic. Typically, APT security systems act as a proxy for client systems to inspect e-mail attachments, URL links, and web-based content to detect and block malicious executables. In this way APT security solutions can even detect zero-day malware based upon the reputation of its source or its behavioral characteristics. Since endpoint systems may be infected when they are used remotely, APT gateways should also be able to respond to C&C traffic based upon URL reputation, DNS behavior, or the specific content within C&C-bound IP packets themselves.
- **Integrate with real-time security intelligence in the cloud.** APT authors are extremely intelligent, ambitious, and creative, changing their tactics regularly to outwit all security defenses. To keep up with changing attack patterns, APT security systems must be supplemented with real-time intelligence from cloud-based systems and researchers. This intelligence should include details on IP address/URL reputation scoring, known web-based files, communications fingerprinting, etc. All APT security technology vendors offer some type of intelligence as part of their products. What's most important here is the scope of the cloud-based intelligence (i.e., what types of threats and vulnerabilities are tracked, geographic coverage, etc.), analysis used (i.e., machine-based analysis, human analysis, etc.), and the degree of integration between security intelligence and actual attack detection/prevention carried out by network-based products.
- **Provide tools for analysis and control.** While most organizations will be content with detecting/blocking attacks, security-conscious enterprises may want to complement threat management with analytics capabilities to document exploit detection, track malware behavior, record the URLs and IP addresses of C&C servers, etc. The best APT security systems will offer standalone data capture and analytics as well as tight integration with leading SIEM platforms.
- **Tie into the security architecture.** Given the urgency of addressing APTs, ESG Research indicates that most large organizations purchase and deploy specific APT security technologies on their networks. While this is the most efficient short-term strategy, APT security systems will need to be part of a more comprehensive security architecture, over time. For example, many APTs begin with e-mail attachments containing malicious code that exploits an application- or system-level vulnerability. APT security technologies should block these attacks while simultaneously working with endpoint security, firewalls, IDS/IPS, SIEM, and e-mail security systems to adjust security policy, enforcement, and ongoing monitoring.

Trend Micro and Deep Discovery

Thus far, APT security solutions have come from a handful of ambitious, creative startups rather than traditional security vendors. Trend Micro has been the exception, and with the recent announcement of its Deep Discovery platform, is enhancing its capabilities in attack detection and intelligence.

According to Trend Micro, Deep Discovery provides network-based real-time visibility, insight, and control to help large enterprises reduce the risk of an APT or other type of targeted attack. Trend is able to back up this claim with a combination of:

- **Deep Discovery Inspector**. This is the actual network appliance that examines network traffic and content to detect and analyze threats using specialized detection engines, custom sandboxing, and event correlation rules that are written and maintained by Trend Micro threat researchers.
- **Deep Discovery Advisor.** As an add-on, Deep Discovery Advisor provides an open scalable platform for expanded threat analysis and intelligence that includes sandboxing and security event collection. The web services interface allows for advanced detection to be integrated into other Trend Micro products such as e-mail security, and also with any third-party product. The advanced analysis capabilities are designed to help speed the assessment, containment, and remediation efforts.
- **Intelligence and Integration.** The Deep Discovery products integrate with Trend's Smart Protection Network (SPN) for reputation services and dynamic black listing of files, URLs, IP addresses, etc, and also to provide customers with threat profile data to help guide risk assessment and remediation. Trend also works with leading SIEM platforms to integrate Deep Discovery intelligence with their collection of log events and flow data. Looking forward, Trend Micro will further integrate Deep Discovery detection with its broad portfolio of enterprise-class products. Trend also plans to use collected threat profiles, create real-time custom signatures, and update a customer's protection in response to a detected targeted attack.

Aside from Deep Discovery alone, Trend Micro's size, product portfolio, and security intelligence have made the company an enterprise security leader. With this stature, CISOs looking for APT security solutions offering immediate and future benefit may be well served by exploring the Trend Micro offerings.

The Bigger Truth

The ESG research presented in this white paper demonstrates some good and bad news with regard to APTs. The good news is that large organizations seem to be paying attention: 47% of executives are taking action, changing processes, and investing in new technologies. The bad news is that large organizations typically address APTs incrementally with marginal changes to existing layers of defense. This activity alone has proven to be inadequate.

Yes, all CISOs should assess their security people, processes, and technologies in order to discover and address areas of weakness. In addition to this, large organizations really need to understand APTs, how they work, and why they are successful. Doing this will shed light on the gaps of their current security infrastructure and further illuminate why security solutions designed for APT protection are really necessary.

The fact is that APTs are pervasive, impacting large organizations in all industries and locations in both the public and private sector. Risks can no longer be ignored or addressed with token changes to the status quo; it's time for immediate action. The most efficient way to proceed is with network-based security tools designed to detect, block, monitor, and analyze APT activity in real-time. The best tools here will offer protection across applications, protocols, and threat vectors; deep analytics for security investigations; and integration with the enterprise security infrastructure and cloud-based security intelligence. Trend Micro is one of few vendors that fit this description.

ESG Enterprise Strategy Group | **Getting to the bigger truth.**