Taking a Lean-Forward Approach to Combat Today's Cyber Attacks

Why Organizations Need Much More Than Fundamental Security Tools

Today's cyber attacks have changed radically from just a few years ago. No longer are they the sole province of opportunistic crooks, online vandals, and digital "hacktivists." Today, advanced cyber attacks are the weapon of choice for organized criminal enterprises and nation-states.

In that shift, broad, scattershot attacks designed for mischief have been replaced with attacks that are sophisticated, targeted, stealthy, and persistent. Known as advanced persistent threats, or APTs, this new generation of attacks springs from well-funded and well-organized threat actors.

These cutting-edge attacks easily bypass traditional defenses such as traditional and next-generation firewalls (NGFW), intrusion prevention systems (IPS), anti-virus (AV), and gateways. Those defenses, built for a previous generation of attacks, rely heavily on malware signatures and known patterns of behavior. That approach leaves these defenses extremely vulnerable to fast-moving, ever-evolving threats that exploit previously unknown, zero-day vulnerabilities. Even sandbox technologies, touted as a fresh approach to security, are constrained by many of the same old flaws.

Why Today's Attacks Require A New Security Posture

Advanced attacks comprise distinct, coordinated stages, and often use multiple attack vectors. They can be delivered through websites, email, files shares, and mobile devices. They can be blended (for example, email-based attacks that contain malicious URLs). And they can exploit application and OS vulnerabilities.

Coordinated attacks typically follow this sequence of events:

- **System exploitation.** Leveraging zero-day exploits or targeted spear-phishing tactics, or sometimes both, advanced attacks can effectively compromise specific systems — the critical first step of the campaign. Because subsequent steps can be encrypted or obfuscated, detecting the exploit phase is critical.

Featuring research from Gartner

- **Malware download.** Once a system has been exploited, the attacker downloads a malicious executable, such as a key logger, Trojan backdoor, password cracker, or file grabber. Just one initial exploit can translate into dozens of infections on the same system.

- **Control established.** When the malware installs, the attacker has cracked the first step to establishing a control point from within your defenses. Once in place, the malware calls out to malicious servers for further instructions. At this point, the criminal has established long-term control over systems.

- **Data exfiltration.** Next, data acquired from infected servers is staged for exfiltration. The criminal may encrypt communication to disguise the assets being transmitted.

- **Lateral movement.** During this phase, the criminal works to move beyond the system initially exploited and begins to move laterally within the target organization.

Leaning Forward: How Fireeye Protects Your Assets

The FireEye Oculus platform combines technology, services, and threat expertise to protect your IT assets like no other security company can. Oculus includes the FireEye NX-, EX-, AX-, and CM-series threat prevention platforms; rich, actionable threat intelligence; and world-class global support and services.

The patented FireEye® Multi-Vector Virtual Execution™ (MVX) engine is the foundation of the FireEye platform. Built from the ground up to combat APTs and other advanced attacks, the MVX engine dynamically analyzes advanced malware in real time. Unlike traditional malware defenses, the MVX engine does not just compare bits of code to signatures. Instead, it captures and confirms zero-day and targeted APT attacks by detonating suspicious files, Web objects, and email attachments within instrumented virtual machine environments. The MVX engine correlates activity across all major threat vectors for a big-picture view of threats — not the narrow, single-flow file analysis most sandboxes provide.

Gain a Cohesive, Correlated View of All Major Threat Vectors—Web, Email, File Shares, and Mobile

The FireEye Oculus platform gives organizations a real-time correlated view of all the major threat vectors that cybercriminals use, including:

- **Web.** Browser-based threats and malicious communications can take many forms and move across a range of protocols, including FTP, HTTP, and IRC. The FireEye NX series tracks sites and communications in real time, across these different protocols to thwart advanced attacks.

- **Email.** Spear-phishing emails represent one of the most common approaches for launching an advanced attack. The FireEye EX series (an on-premise appliance) and Email Threat Prevention (a cloud-based solution) can guard against these types of threats. They provide real-time analysis of URLs in emails, email attachments, and Web objects to determine whether they are malicious.

- **File Shares.** Even if Web and email channels are secured, malicious files can still make it into an organization's network in any number of ways — through a USB drive, a mobile device, download from a cloud service, and many more. The FireEye FX series detects and eliminates malware hiding in file shares and content repositories.

- **Mobile.** Mobile malware can do everything from exfiltrate sensitive data to secretly record video and audio. FireEye Mobile Threat Prevention analyzes suspicious mobile apps to detect and stop malicious or unwanted behavior.

Leaning Farther Forward with Local and Global Intelligence and Continuous Monitoring

Suspicious objects singled out by the NX, EX, and FX platforms can be thoroughly analyzed by the FireEye AX series for forensics. The AX series provides hands-on control over powerful, auto-configured test environments. Security professionals can safely execute and inspect advanced malware, zero-day, and targeted APT attacks embedded in common file formats.

Tying all these pieces together, the FireEye CM series correlates threat intelligence generated by the FireEye NX, EX, and FX platforms automatically and in real time. The network-based CM platform distributes this intelligence to other FireEye products — and even legacy security tools. By coordinating this intelligence and connecting the dots of an attack, the entire organization is protected from targeted attacks.

FireEye users also benefit from the FireEye Dynamic Threat Intelligence™ (DTI) cloud, which shares anonymized threat intelligence from participating FireEye deployments around the globe. This worldwide cloud-based platform efficiently shares information about emerging threats and new threat findings from FireEye Labs.

Finally, FireEye Oculus Continuous Monitoring provides real-time threat monitoring that leverages superior threat intelligence, global services, and research. The FireEye team, which includes some of the industry's top cyber analysts, constantly monitors subscribed systems for advanced attacks — not just in your organization, but other organizations in your industry or region - and proactively notifies subscribers of malicious activity.

Oculus Continuous Monitoring provides actionable, in-depth analysis of real-world outbreaks and advanced, bleeding-edge research. Diving deeper into potential threats, Oculus Continuous Monitoring helps identify attackers seeking to steal your information assets. Learn about emerging threats and fine-tune your defense before they get the chance to strike.

Source: FireEye

[1]Yacin Nadji, et al. "Automated Remote Repair for Mobile Malware." December 2011.
[2]Josh Halliday. "App for Google Android smartphones secretly records calls." August 2011.

Research from Gartner

Strategies for Dealing With Advanced Targeted Attacks

Targeted attacks, often called APTs, penetrate existing security controls, causing significant business damage. Enterprises need to focus on reducing vulnerabilities and increasing monitoring capabilities to deter or more quickly react to evolving threats.

Key Challenges

- The term "advanced persistent threat" (APT) has been overhyped in the press, distracting organizations from evolving their security controls and processes.
- The major advance in new threats has been the level of tailoring and targeting.
- Advanced threats are using targeted attacks to get past standard levels of security controls.
- Poor security practices and unmonitored employee behaviors can undermine the efficiency of advanced threat detection technologies.

Recommendations

- Assess your existing defenses and identify missing or obsolete layers and unmonitored systems.
- Focus on upgrading critical security processes regarding vulnerability management, continuous monitoring, and incident response to reduce the attack surface and potential damages.
- Plan for the implementation of "lean-forward" solutions and processes to deter or rapidly react to advanced threats.
- Put equal efforts on processes and technologies when mitigating APTs.

Introduction

The term "advanced persistent threat" was coined by the U.S. military to refer to a specific threat actor (China). It was expanded to include other aggressive nation states, but has been co-opted by the media and by security vendors to hype the source of an attack. This distracts from the real issue — focusing on the vulnerabilities that the attackers are exploiting.

Advanced Persistent Threat and Advanced Targeted Attacks

Gartner uses a simple definition for "APT":

- **Advanced:** It gets through your existing defenses.
- **Persistent:** It will keep trying until it gets in, and once done, it succeeds in remaining hidden from your current level of detection until it attains its objective.
- **Threat:** It can cause harm.

We think the targeted aspect is more important to focus on. These are not noisy, mass attacks that are easily handled by simple, signature-dependent security approaches. That's why, for the purposes of this research, we will use the term "advanced targeted attack."

As business use of the Internet evolves, the threats also continue to evolve. It wasn't that long ago that simple website defacement attacks and denial-of-service incidents were the most damaging forms of attack. However, starting in 2008 or so, we began to see the growth of financially motivated targeted attacks. Targeted attacks are a much higher risk to the bottom line, and are generally launched by more-sophisticated attackers who are motivated to penetrate defenses quietly to get inside and steal information — for as long as possible. This maximizes their revenue opportunities. These same techniques were already used by politically motivated attackers (evidence suggests that Stuxnet was already operating in 2005).[1] The reality is that the most important issues are the vulnerabilities and the techniques used to exploit them, not the country that appears to be the source of the attack. Gartner estimates that, for the average enterprise, 3% to 5% of its endpoints are compromised at any time.

The major advance in new threats has been the level of tailoring and targeting. Targeted attacks aim to achieve a specific impact against specific enterprises, and have three major goals:

- **Information compromise:** Stealing, destroying or modifying business-critical information

- **Theft of service:** Obtaining use of the business product or service without paying for it
- **Denial of service:** Disrupting business operations

The motivation for advanced targeted attacks is usually financial gain, such as through extortion during a denial-of-service attack, trying to obtain "ransom" for stolen information, or selling stolen identity information to criminal groups. This is not to say that state-sponsored attacks do not occur, because they do. Many state-sponsored attacks have been very clever. However, in the majority of cases, they are using attack techniques that were first seen in financially motivated attacks (Stuxnet is probably one of the few exceptions). Some of the state-sponsored attacks exploited "zero-day" vulnerabilities that weren't seen before, but financially motivated targeted attacks have done that for years.

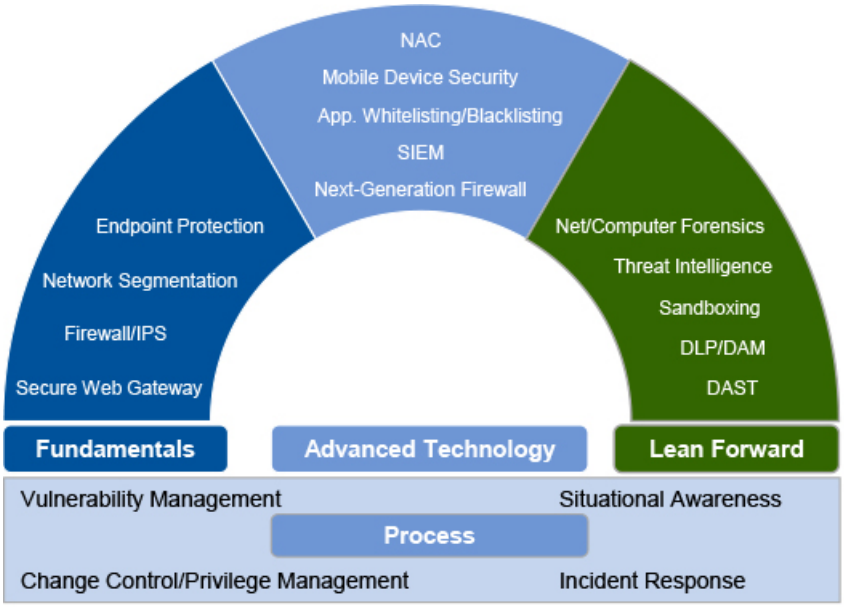
Analysis

Embrace a "Lean Forward" Approach to Security

Targeted attacks often use custom-created malware that is undetectable by signature-based techniques. To be successful, such attacks generally require some means of communication back to an outside party, whether out of band (as when an insider puts information onto removable media and physically carries it outside of enterprise control) or in band (as when Internet mechanisms are used in modern botnet-style threats). One key to preventing success by the attackers is to focus on avoiding, minimizing or shielding the vulnerabilities they are exploiting.

Because software and people will always be vulnerable (see Note 1), we will always need defenses to mitigate vulnerabilities. However, in 2013, we are in one of those periods that occurs every five years or so (see Note 2), where the attackers find new levels of vulnerabilities to exploit, and the threats get ahead of the standard level of protection. When that happens, Type A (technically aggressive) organizations need to react quickly to upgrade defenses in a lean-forward manner, because they often have the most to lose, while Type B (mainstream) and Type C (technologically conservative) organizations will often only be able to take less-aggressive measures or wait for standard product offerings to offer more-effective capabilities (see Figure 1 for examples of available technologies).

FIGURE 1 Defending Against Targeted Attacks Requires Lean-Forward Technologies and Processes



DAM = digital asset management; DAST = dynamic application security testing; DLP = data loss prevention; IPS = intrusion prevention system; NAC = network access control; SIEM = security information and event management
Source: Gartner (June 2013)

Enterprises should not take compliance with security standards as a sufficient objective. There is a big difference between compliance and security. Sufficient controls from a compliance point of view are simply limiting the company's liability from legal action — it is never a sufficient answer to dealing with advanced threats. This requires strong processes and careful planning and prioritization, because organizations scan and discover vulnerabilities much faster than they can patch them.

Process

Focus on processes and how they influence employees' behavior. As part of process improvement, Gartner recommends focusing on high-priority security processes and emphasizing improving the effectiveness of vulnerability management, control/configuration management programs and incident response.

Many attacks that include zero-day exploits often use well-known vulnerabilities as part of the overall attacks. If you close the vulnerability, then you could stop the curious teenager, the experimental hacker, the cybercriminal and the information warrior. For example, for Stuxnet to succeed, it exploited a well-known, hard-coded password, and the fact that USB drivers were regularly used to transfer data to and from nuclear power plant control networks. Closing or shielding some well-known vulnerabilities would have made Stuxnet much less likely to succeed. In a similar way; password thefts at Sony (2011), Yahoo (450,000 emails and passwords published in 2012), DropBox (2012) and Evernote (2013), were all possible because of poorly implemented security practices. More information on how to improve these practices is available in "The Security Processes You Must Get Right."

Social engineering is one of the key techniques used to get into a system that security technologies can't prevent. However, traditional security awareness programs fail to improve enterprise security. Stimulating and maintaining employee behavior that supports enterprise security requires new techniques drawn from the world of advertising and behavior management.

Fundamentals

Firewalls, intrusion prevention systems (IPSs), secure Web gateways (SWGs) and endpoint protection platforms (EPPs) are fundamental security technologies. Network segmentation is another fundamental component that enhances security, and serves to reduce the cost and scope of compliance audits. When combined with the security processes we have outlined (for example, vulnerability management and change management), these core components provide a base level of threat protection. However, because advanced threats are able to bypass these fundamental defenses, security-conscious organizations must implement some advanced technologies and consider lean-forward solutions.

Advanced Technology

Most Type A, and many Type B, enterprises will find that the risks to their businesses are too high to ignore, and they should take steps to strengthen their environments beyond the basic level. To reach an acceptable level of security in 2013, security information and event management (SIEM) products, or other approaches that correlate information across defense "silos," should be used to gain better exception monitoring capabilities. More-advanced techniques — such as whitelisting, sandboxing and proactive application vulnerability testing prior to deployment — should also be employed to deny advanced targeted attacks the ability to install executables on servers and PCs. Smartphones and tablets should also get specific attention to avoid the common pitfalls for mobile security.

Lean Forward

Businesses and government agencies involved in critical infrastructure, high-tech or financial operations, which are constant targets of cybercrime and other advanced threats, need to add lean-forward capabilities to have continual visibility into potential attacks and compromises. A lean-forward approach to security is going beyond the standard level of the network security and vulnerability assessment controls, and using tools and processes to continuously look for active threats on internal networks The use of specialized detection techniques (system emulation and heuristics), network forensics, and situational awareness technologies can be very effective in quickly detecting and reacting to the first stages of an advanced targeted attack, but require high levels of skilled resources to be effective. The real key is avoiding as many attacks as possible, and more rapidly reacting to those that just can't be avoided.

All the lean-forward tools discussed here are available as point products, but subsets of their functionality will be absorbed into other network security platforms and will be good enough for many enterprises. For example, most SIEM and next-generation firewall products have added some of the flow analysis features of network behavior analysis. Leading SWG and next-generation firewall vendors embed reputation services, application awareness and other features of specialized advanced threat detection products. Many advanced vulnerability testing products are adding "seek, refine, repeat" functions that provide some aspects of penetration testing. The digital forensics area (computer plus network forensics) will likely stay in its own market, but many features will be available from SIEM products

Adding lean-forward tools from the samples listed in Figure 1 will reduce risk, but also requires new or changed processes and controls. These tools generally will require higher investments in acquisition and staffing, but will also provide a higher payoff in the effectiveness of detecting advanced threats, and support more-rapid tuning or enhancement of network-based security controls.

Evolve Security Practices; Don't Just Add Technology Layers

Having more security layers does not automatically mean more-effective security. New security solutions should augment good security practices. In the real world, many security budgets do not support what translates into, "Keep spending on what you were spending on, and spend on more new stuff, too." The high visibility and economic impact of the incidents at other companies can often be used to convince management to support more-stringent policies and controls in these areas, with little need to increase budgets. One important upgrade to these processes is moving toward more continuous monitoring versus yearly or quarterly auditing.

A lean-forward, continuous monitoring process consists of these steps:

1 Assessing and verifying the scope of monitoring systems

2 Updating threat information

3 Monitoring, inspecting and correlating network traffic and host logs

4 Investigating possible threat activity

5 Initiating an incident response process

6 Updating defenses or work-arounds

7 Adapting and monitoring incident response processes

8 Going back to Step 1

The best approach to reducing the risk of compromise is always "security in depth" — if you can afford it. Affording it means not just the money to buy increasing numbers of security products, but also the staff and operations support to use and integrate everything together. New monitoring tools require additional teams to take care of alerts; Next-generation firewalls can only detect attacks that pass through them; however, they cannot prevent employees from giving their credentials to a stranger on the phone. That's why good security practices play an equally important role in the security improvement process.

Starting Points

To ensure that businesses are protected from advanced targeted attacks, they must first start from a solid baseline:

- What is the current level of security program maturity in dealing with standard levels of attacks?
- Are you exposed to specific risks?
- Do you miss any fundamental tool or process?

Where gaps are identified that require an upgrade or a change to security controls and processes, incorporate some of the lean-forward capabilities (through products or services) detailed here to evolve security defenses to get ahead of (or at least stay even with) evolving advanced targeted attacks.

Evidence

Note 1. Key Issues in Addressing Advanced Threats

Because enterprises can never completely avoid vulnerabilities, the Recommended Reading section points to a number of Gartner documents that detail other key security capabilities. Future Gartner research will expand on this area.

Note 2. Periods of Vulnerability

From 2001 through 2003, worms that exploited vulnerabilities in Microsoft Windows got ahead of protection, driving advances in intrusion prevention systems, just as in 1995, advances in macroviruses drove advances in antivirus protection, and phishing attacks in 2006 drove advances in email security. The same thing has been happening since 2011, with advanced targeted attacks leading to advances in anti-malware, intrusion prevention and network forensics.

Gartner RAS Core Research Note G00252555,
Jeremy D'Hoinne, Lawrence Orans, 6 June 2013

About FireEye

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors, including Web, email, and files and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 1,300 customers across more than 40 countries, including over 100 of the Fortune 500.

For more information, visit: www.FireEye.com.