FireEye™

White Paper

Advanced Targeted Attacks

How to Protect Against the Next Generation of Cyber Attacks

Contents

Executive Summary

The new threat landscape has changed. Cybercriminals and nation-states are aggressively pursuing valuable data assets, such as financial transaction information, product design blueprints, user credentials to sensitive systems, and other intellectual property. Simply put, the cyber offense has outpaced the defensive technologies used by most companies today.

Next-generation firewalls, intrusion prevention systems (IPS), anti-virus, and security gateways are not adequately protecting organizations from next-generation threats. With over $20B spent annually on IT security, nearly all of it is spent on outdated, signature-based technology. Signature-based defenses only stop known threats, not the unknown, dynamic attacks being used today. This is why over 95% of companies harbor advanced malware within their network despite the many layers of traditional defenses organizations have deployed.

Cybercriminals are armed with the latest zero-day vulnerabilities, commercial-quality toolkits, and social engineering techniques to perpetrate advanced targeted attacks. These threats move "low and slow" and use several stages and channels to duck traditional defenses and find vulnerable systems and sensitive data. As a result, defending against these attacks requires a strategy that moves beyond static signatures and rudimentary behavioral heuristics.

Traditional defenses are increasingly becoming policy enforcement points rather than robust defenses against cyber intrusions. For example, URL filters are still useful for enforcing acceptable use policies around employee Web surfing, but no longer effective at defending against dynamic drive-by download attacks. Likewise, next-generation firewalls (NGFW) simply add next-generation policy options around users and applications and consolidate traditional signature-based protections. While NGFW may consolidate traditional AV and IPS protections, these are signature-based technologies and they do not add new levels or innovations to defending networks. Integrating together these traditional defenses do little to thwart next-generation threats.

Against dynamic threats, traditional defenses like firewalls, IPS, anti-virus, anti-spam, and security gateways collapse, leaving a wide-open hole for cybercriminals. Today's attacks utilize advanced tactics, such as blending polymorphism and personalization, to appear unknown to signature-based tools and yet authentic enough to bypass spam filters and even fool targeted victims. For example, spear phishing attacks leverage social networking sites to craft personalized emails that deliver dynamic, malicious URLs that bypass URL filters.

To regain the upper hand against next-generation attacks, enterprises must turn to true next-generation protection: signature-less, proactive, and real-time. Through continuous analysis of suspicious code throughout the attack lifecycle and blocking of malware communications across multiple threat vectors, next-generation protections can stop advanced malware, zero-day exploits, and advanced persistent threat (APT) tactics from threatening sensitive data assets.

"There is widespread agreement that advanced attacks are bypassing our traditional signature-based security controls and persisting undetected on our systems for extended periods of time. The threat is real. You are compromised; you just don't know it."

– Gartner, Inc., 2012

Nature of Next-Generation Threats

Attacks have changed in form, function, and sophistication from just a few years ago. Next-generation threats utilize both mass-market malware designed to infect many systems as well as sophisticated, zero-day malware to infect targeted systems. They blend multiple attack vectors cutting across Web, email, and application-based attacks. And today's attacks are aimed at getting valuable data assets—sensitive financial information, intellectual property, authentication credentials, insider information—and each attack is often a multi-staged effort to infiltrate networks, spread, and ultimately exfiltrate the valuable data.

From the common Zeus/Zbot infections to the targeted Stuxnet malware, cyber attacks have proven effective at stealing sensitive data, causing financial loss, and damaging corporate reputations. Cybercriminals are transacting billions of dollars in cyber activities. Nation-states are using malware in cyber espionage to spy on opposition activists and disrupt adversary's critical infrastructure. Because of the high stakes, zero-day exploit development and other criminal activities are well funded. This has led to an active underground ecosystem that trades and sells access to systems residing within some of the most sensitive networks in the world. Cyber operations such as GhostNet, Night Dragon, and Nitro have affected global corporations and governments using targeted APT tactics, spear phishing, and advanced malware.

Every organization in the information "supply chain" is at risk of attack. For example, the March 2011 theft of two-factor authentication algorithms from RSA (a division of EMC) shows the strategic nature of these attacks: the intellectual property they stole from RSA "could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack,"[1] allowing criminals to break in at enterprises around the world.

In April 2012, VMware (a subsidiary of EMC) confirmed that a hacker had publicly released a portion of VMware's source code dating to 2003 and 2004. With more data centers utilizing virtualization, "a November 2010 IBM study[2] analyzed virtualization and hypervisor security vulnerability disclosures over the past decade from Citrix Systems, IBM, Microsoft, Oracle, Red Hat, and VMware. It indicates that 35% of the security vulnerabilities allow an intruder to escape from a guest virtual server to affect other virtual servers or the hypervisor."[3] These are just two examples of advanced targeted attacks seeking valuable intellectual property to be used in further APT attacks.

"Organizations face an evolving threat scenario that they are ill-prepared to deal with."

– Gartner, Inc., 2012

"APT attackers are more highly motivated. They're likely to be better skilled, better funded, and more patient. They're likely to try several different avenues of attack. And they're much more likely to succeed."[4]

1 http://www.rsa.com/node.aspx?id=3872

2 http://public.dhe.ibm.com/common/ssi/ecm/en/wgl03007usen/WGL03007USEN.PDF

3 http://searchservervirtualization.techtarget.com/tip/Virtualization-and-hypervisor-security-vulnerabilities-to-look-out-for

4 http://www.schneier.com/blog/archives/2011/11/advanced_persis.html

The Five Stages of Multi-Vector, Multi-Stage Attacks

Next-generation threats are complex, cutting across multiple attack vectors to maximize the chances of breaking through network defenses. Multi-vector attacks are typically delivered via the Web or email. They leverage application or operating system vulnerabilities, exploiting the inability of conventional network-protection mechanisms to provide a unified defense.

In addition to using multiple vectors, advanced targeted attacks also utilize multiple stages to penetrate a network and then extract the valued information. This makes it far more likely for attacks to go undetected. The five stages of the attack lifecycle are as follows:

Stage 1: System exploitation. The attack attempts to set up the first stage, and exploits the system using "drive-by attacks" in casual browsing. It's often a blended attack delivered across the Web or email threat vectors, with the email containing malicious URLs.

Stage 2: Malware executable payloads are downloaded and long-term control established. A single exploit translates into dozens of infections on the same system. With exploitation successful, more malware executables—key loggers, Trojan backdoors, password crackers, and file grabbers—are then downloaded. This means that criminals have now built long-term control mechanisms into the system.

Stage 3: Malware calls back. As soon as the malware installs, attackers have cracked the first step to establishing a control point from within organizational defenses. Once in place, the malware calls back to criminal servers for further instructions. The malware can also replicate and disguise itself to avoid scans, turn off anti-virus scanners, reinstall missing components after a cleaning, or lie dormant for days or weeks. By using callbacks from within the trusted network, malware communications are allowed through the firewall and will penetrate all the different layers of the network.

Stage 4: Data exfiltration. Data acquired from infected servers is exfiltrated via encrypted files over a commonly allowed protocol, such as FTP or HTTP, to an external compromised server controlled by the criminal.

Stage 5: Malware spreads laterally. The criminal works to move beyond the single system and establish long-term control within the network. The advanced malware looks for mapped drives on infected laptops and desktops, and can then spread laterally and deeper into network file shares. The malware will conduct reconnaissance: it will map out the network infrastructure, determine key assets, and establish a network foothold on target servers.

"An attacker who has compromised an account holder's PC can control every aspect of what the victim sees or does not see, because that bad guy can then intercept, delete, modify or reroute all communications to and from the infected PC."[5]

5 http://krebsonsecurity.com/2011/02/sold-a-lemon-in-internet-banking/

The Price of The Problem

Enterprises pay a high operational price. A 2012 InformationWeek survey found that in 2011 over a quarter of companies surveyed spent at least 10% to over 25% of their annual IT budget on security alone.[6] "Phishing and malware make a powerful team. According to our [InformationWeek] survey, malware remained the No. 1 breach type that our respondents experienced."[7]

The 2011 Ponemon Cost of a Data Breach survey found that "the pattern of results in 2011 is consistent with prior years, when the most costly breaches typically involve malicious acts against the company rather than negligence or system glitches."[8] "What's more, these data breaches are the most expensive. Malicious attacks create more costs because they are harder to detect, the investigation is more involved, and they are more difficult to contain and remediate."[9]

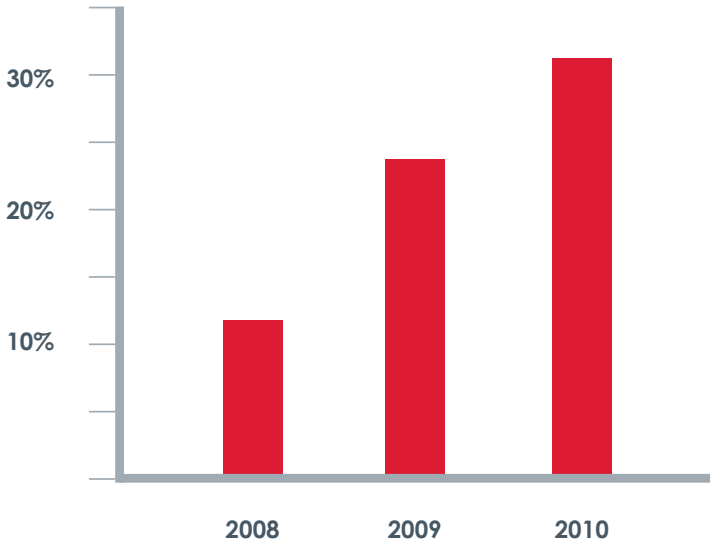

Figure 1: Malicious attacks are the root cause of an increasing percentage of data breaches. Source: Ponemon

6 InformationWeek's 2012 Strategic Survey. Page 34.

7 Ibid. Page 16

8 2011 Cost of Data Breach Study - United States. Benchmark Research Conducted by Ponemon Institute LLC. Report: March 2012. http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide__CODB_US

9 http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher

How Next-Generation Threats Bypass Traditional Security

Next-generation threats happen over multiple stages across several threat vectors when penetrating a network and then extracting valued information. Cybercriminals combine Web, email, and file-based attack vectors in a staged attack, making it far more likely for their attacks to go undetected. Today's firewalls, IPS, anti-virus, and Web gateways have little chance to stop attackers using zero-day, one-time-use malware, and APT tactics.

These blended, multi-stage attacks succeed because traditional security technologies rely on fairly static signature-based or list-based pattern matching technology. Many zero-day and targeted threats penetrate systems by hiding newly minted, polymorphic dropper malware on innocent Web pages and in downloadable files like JPEG pictures and PDF documents. Or they use personalized phishing emails sent to carefully selected victims with a plausible-looking message and malicious attachment targeting a zero-day vulnerability. Or they troll social media sites embedding tweets that include a shortened URL masking the malicious destination. Each time a victim visits the URL or opens the attachment, a malware payload installs on the victim's computer. This malware code often includes exploits for multiple unknown vulnerabilities in the OS, plug-ins, browsers, or applications to ensure it gains a foothold on the system. "Internet Explorer 6 on Windows XP? I have an exploit for that."

Beyond exploit technological advantages, cybercriminals also realize they can divide and conquer because that is how traditional defenses and IT departments are organized. Traditional security defenses are typically set up to inspect each attack vector as a separate path and each stage as an independent event, rather than viewing and analyzing the stages and vectors as an orchestrated series of cyber incidents. By exploiting the technological and business silos within IT departments, a drive-by Web infection looks like a random event blamed on an end-user's poor decision to visit a dubious website. It cannot be traced back to the originating spear phishing email used to fool the user and initiate a multi-stage advanced targeted attack. So, after multiple stages of attacks across Web and email, cybercriminals are able to exfiltrate data without defenders finding out until far too late.

"Incumbent defenses fall short…existing anti-malware initiatives are no longer enough."
– Forrester Research, Inc., 2011

"RSA was hacked some time in the first half of March when an employee was successfully spear phished and opened an infected spreadsheet. As soon as the spreadsheet was opened, an advanced persistent threat (APT)—a backdoor Trojan—called Poison Ivy was installed. From there, the attackers basically had free reign of RSA's internal network, which led to the eventual dissemination of data pertaining to RSA's two-factor authenticators."[10]

10 http://downloadsquad.switched.com/2011/04/06/security-firm-rsa-attacked-using-excel-flash-one-two-sucker-punc/

How Do Next-Generation Threats Get Past Traditional Barriers?

- **Firewalls:** Firewalls allow generic http Web traffic. Next-generation firewalls (NGFW) add layers of policy rules based on users and applications. NGFW consolidate traditional protections such as anti-virus and IPS but do not add dynamic protection that can detect next-generation threat content or behavior.
- **IPS:** Signatures, packet inspection, DNS analysis, and heuristics will not detect anything unusual in a zero-day exploit, especially if the code is heavily disguised or delivered in stages.
- **Anti-virus and Web malware filtering:** Since the malware and the vulnerability it exploits are unknown (zero-day), and the website has a clean reputation, traditional anti-virus and Web filters will let it pass. The volume of vulnerabilities in browser plug-ins like Adobe and the exponential combinations of these browsers with operating systems make it hard for anti-virus vendors to keep up.
- **Email spam filtering:** Spoofed phishing sites use dynamic domains and URLs, so blacklisting lags behind criminal activities. It takes more than two days to shut down the average phishing site.[11]

Malicious code can also be carried in on laptops, USB devices, or via cloud-based file sharing to infect a machine and spread laterally when it connects into the network. It is common for mobile systems to miss updates to DAT files and patches, so they are vulnerable to both known and unknown exploits. In general, even up-to-date machines can be infected using zero-day exploits and social engineering techniques, especially when the system is off the corporate network.

Once in place, malware may replicate itself—with subtle changes to make each instance look unique—and disguise itself to avoid scans. Some will turn off anti-virus scanners, reinstall after a cleaning, or lie dormant for days or weeks.

Eventually, the code will phone home to the criminal for further instructions, a new payload or to deliver login credentials, financial data, and other valuables. Many compromised hosts provide a privileged base so the criminal can explore further or expand his botnet with new victims.

Most companies don't analyze outbound traffic for these malicious transmissions and destinations. Those organizations that do monitor outbound transmissions use tools that look for "known" bad actor addresses and regulated data.

- **Web filtering:** Most outbound filtering blocks adult content or time-wasting entertainment sites. Less than a quarter of enterprises restrict social networking sites.[12] In addition, dynamic URLs, hacks of legitimate websites, and addresses that are active for brief periods make static URL blacklisting obsolete.
- **Data loss prevention (DLP):** DLP tools were primarily designed for personally identifiable information (PII)—strings like social security numbers, license numbers, or health data—and these tools are only as good as their rules. Most are too coarse-grained and cumbersome to detect exfiltration of credentials or intellectual property. Encryption of callback channels allows data to escape unseen. Their static approach does not match the dynamic nature of next-generation threats.

11 Source: Symantec, 2010

12 The Sophos survey stated, "More than half of the companies surveyed imposed no limitations on accessing Facebook, Twitter and LinkedIn—and less than a quarter of firms completely block these sites." https://secure.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-2011-wpna.pdf

Plugging The Security Hole

The gap in protection and the increased sophistication of cybercriminals call for a new category of threat prevention tools adapted to the resilient, evasive, and complex nature of next-generation threats. This is why security-conscious organizations choose FireEye for industry-leading protection against next-generation threats that cut across multiple threat vectors and use multiple stages to systematically bypass traditional defenses. FireEye Malware Protection System (MPS) supplements traditional and next-generation firewalls, IPS, AV, and gateways, whose signatures and heuristics cannot stop this next generation of threats.

The FireEye MPS appliances have been designed to protect across the Web and email threat vectors and malware resident on file shares. It is an integrated security platform offering multi-vector protection and stops all stages of an advanced attack. Each of FireEye's security appliances features the Virtual Execution (VX) engine that provides state-of-the-art, signature-less analysis using patented, proprietary virtual machines. The Malware Protection System builds a 360-degree, stage-by-stage analysis of an advanced attack, from system exploitation to data exfiltration, in order to most effectively stop would-be APT attackers.

Operating inline or out of band, FireEye Malware Protection System perform automated, real-time analysis of suspicious Web traffic, email attachments, and files on network file sharing servers. Anything that looks suspicious is executed in the VX engine where the proprietary, full-fledged testing environments confirm irrefutably the maliciousness and activities of the attacker, zeroing in on real threats and avoiding false positives and false negatives.

Once misbehaving code is flagged, its communication ports, IP addresses, and protocols are blocked to shut down outbound transmissions. Analysts can use the fingerprint of the malicious code surgically to identify and remediate compromised systems and prevent the infection from spreading. Forensics researchers can run files individually through automated offline tests to confirm and dissect malicious code. Shared cloud-based threat intelligence keeps everyone up to date on the cybercrime innovations and callback destinations being identified at FireEye Labs and other customer sites.

These turnkey Web, email, and file share protection appliances deploy in under 30 minutes, with no rules to write or tune. And the purchase price starts at a tiny fraction of the cost of a data breach.

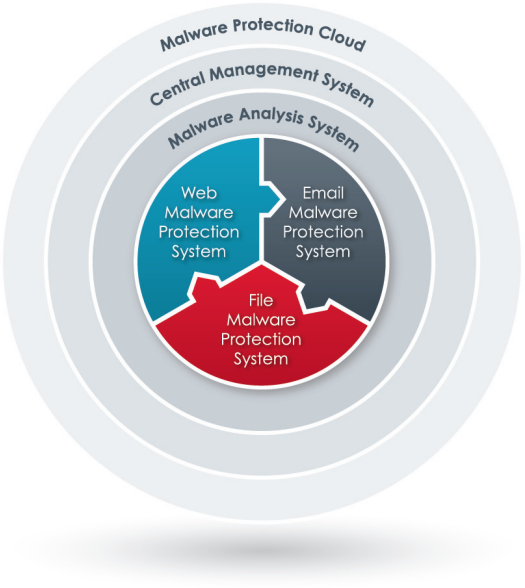

Figure 2: Complete protection against advanced targeted attacks

Next-Generation Security to Stop Advanced Attacks

The FireEye Malware Protection System plugs the network hole left wide open in virtually every organization today. Featuring the patent-pending VX engine, the FireEye MPS dynamically generates security content to stop previously unknown attacks coupled with dynamic code execution to detect the zero-day threats. Companies can now have true real-time inbound and outbound protections against advanced targeted attacks.

Enterprises of all sizes can reinforce their traditional defenses with next-generation threat prevention that understands the nature and intent of these malicious, advanced targeted attacks, especially those bearing the hallmark of the advanced persistent threat. Sign up today for a FireEye security evaluation of your network to see the threats getting through your current protections.

About FireEye, Inc.

FireEye, Inc. is the leader in stopping next-generation threats that use advanced malware, zero-day exploits, and APT tactics. FireEye solutions supplement traditional and next-generation firewalls, IPS, anti-virus, and gateways, which cannot stop advanced threats, leaving security holes in networks. FireEye offers the industry's only solution that detects and blocks attacks across Web and email threat vectors as well as malware resident on file shares. It addresses all stages of an attack lifecycle with a signature-less engine utilizing stateful attack analysis to detect zero-day threats. Based in Milpitas, California, FireEye is backed by premier financial partners including Sequoia Capital, Norwest Venture Partners, and Juniper Networks.

Learn more at www.fireeye.com

FireEye, Inc. | 1390 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.fireeye.com