FireEye™

White Paper

CISO Guide to Next Generation Threats

Combating Advanced Malware, Zero-Day and Targeted APT Attacks

Table of Contents

FireEye™

White Paper

Introduction

Over 95% of businesses unknowingly host compromised endpoints, despite their use of firewalls, intrusion prevention systems (IPS), antivirus and Web gateways.[1] This situation—the new status quo—results from criminals leveraging multiple zero-day vulnerabilities, commercial-quality toolkits and social media to perpetrate next-generation threats. These threats move "low and slow" and use several stages and channels to duck traditional defenses and find vulnerable systems and sensitive data.

Defending against next-generation threats requires a strategy that moves beyond signatures and behavioral heuristics. Signatures and heuristics remain valuable against known threats: criminals never throw away an exploit toolkit or other penetration technique, they just add new capabilities and concoct new evasion tactics. But against unknown threats, traditional defenses like firewalls, IPS, antivirus and Web gateways collapse, leaving a wide-open hole for cybercriminals. Today's attacks look new and unknown to signature-based tools because the attacks employ advanced malware and zero-day vulnerabilities. These attacks do not trigger heuristics because of techniques like camouflage, multi-stage packaging, targeting and other advanced persistent threat (APT) tactics.

Next-generation firewalls add next-generation policy options around users and applications and consolidate traditional signature-based protections. They may consolidate traditional AV and IPS protections. But they are not adding new levels or innovations to these protections, so they do nothing to thwart next-generation threats.

To regain the upper hand against next-generation attacks, enterprises must turn to true next-generation protection: signature-less, proactive and real time. Through constant testing of any suspicious code and blocking of communications with malicious hosts, next-generation protections combat advanced malware, zero-day and targeted APT attacks that bypass defenses like next-generation firewalls, IPS, antivirus, and Web gateways.

The Moving Target: From PII to IP Credentials

In the 2011 CyberSecurity Watch Survey, 28% of respondents reported an increase in the number of cybersecurity events.[2] Understanding the criminal's motivation helps us understand his determination —and "deep pocket" investment in malware development and infrastructure such as bot networks. For the last decade or so, regulations have forced IT teams to wrap controls around financial and personally identifiable information (PII).

Combined with more sophisticated fraud detection, the street price of basic credit card and identity data has fallen to unprofitable levels. Margins have also evaporated on generic phishing of bank

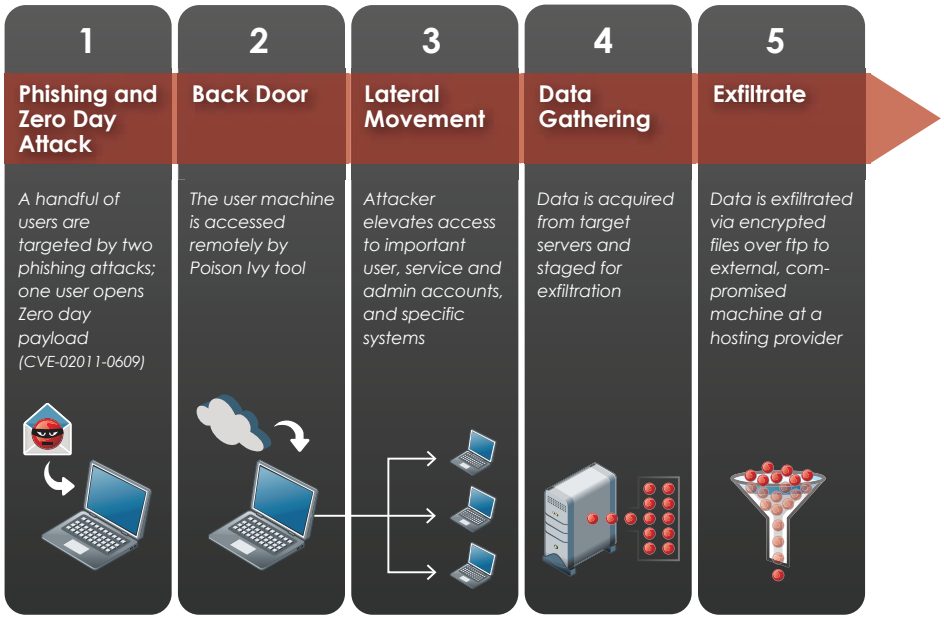
In early 2011, email that included malware spiked to 30% of all email received, while phishers flocked to Website categories including games, health and medicine and portals.[3]

Websites and eBay. In search of profits, ever-resilient criminals have adapted their attack techniques from generic and indiscriminate to personalized and targeted.

Attackers continue to pursue personally identifiable information, as demonstrated by the theft of email addresses at Epsilon marketing, but now this information is used in targeted personalized emails that lure businesses and consumers to click and download malware. Spam and spear phishing are the first salvo in a coordinated series of steps that result in successful network compromises and data theft.

> **"It's a spammer's fantasy come true. The criminal gets client email addresses along with the names of companies those people do business with—all you need for a targeted "spear phishing" attack… They take over their corporate accounts and then use them to send spam—often fake Skype or Adobe reader updates that actually contain malicious software."[4]**

The big cybercrime market opportunity today is for intellectual property (IP) and bank and enterprise credentials. The March 2011 theft of two-factor authentication data 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,"[5] allowing criminals to break in at enterprises around the world.



Next-generation threats like the RSA attack use successive inbound and outbound stages

"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."[6]

These attacks, like the Operation Aurora source code thefts at Symantec, Google, Adobe, Intel and Morgan Stanley, have gone after IP. They used multiple stages and avenues to enter the network and navigate to the data that had value. Many of them incorporated personal data gleaned from social media, as well as zero-day vulnerabilities. The first item of value stolen was often access credentials. Stolen credentials can open the doors to administration of the database, Web or email server. [7] If it is the CFO's credential, it can be the authentication required to take over and withdraw funds from the corporate bank account.

> **"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 re-route all communications to and from the infected PC." [8]**

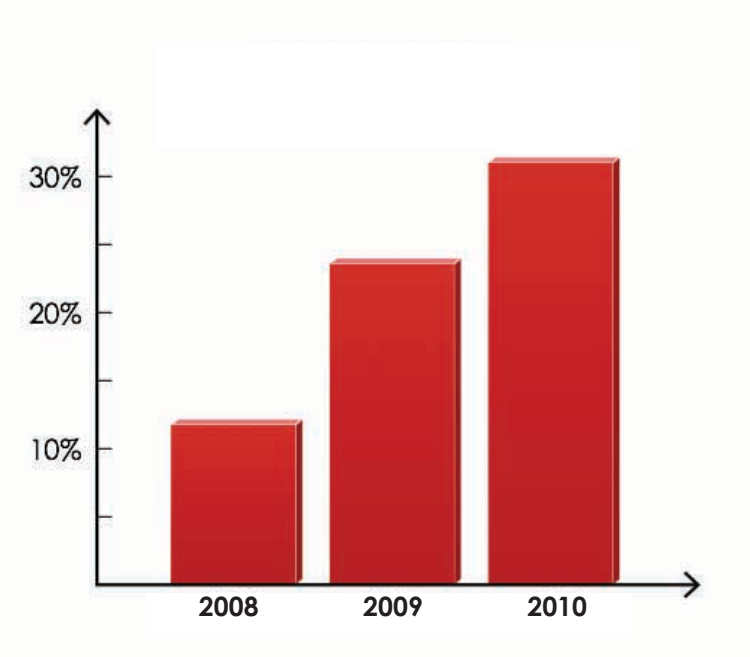
From Big Business to Every Business

Today's versatile, drag-and-drop toolkits allow criminals endless permutations of attack options, pursuing smaller businesses as the larger organizations improve their defenses. Every business has a bank account, a customer database, a product design, or some other asset of value. Even if no data is stolen, every compromised system can add free compute cycles to a spam botnet.[9]

Criminals reuse successful techniques wherever they can turn a profit. Often, it's the same tactic, just a different avenue of attack. A Sophos survey of 2010 cybercrime showed social networking users started receiving more malware and spam. Two-thirds of respondents had experienced spam via social networks, and four out of 10 had received malware from these sites. Phishing attacks rose steeply from 30% to 43%, and new malware appears about once a second.[10]

The Price of The Problem

Enterprises pay a high operational price. Malware detection and analysis and incident response take up more than half of IT Security professionals' time.[11] "Malicious attacks were the root cause of 31 percent of the data breaches studied. This is up from 24 percent in 2009 and 12 percent in 2008," according to the 2011 Ponemon Cost of a Data Breach survey. "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."[12]



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

How Next-Generation Threats Bypass Traditional Security

Today's firewalls, IPS, antivirus, and Web gateways have little chance to stop attackers using zero-day, one-time-use malware and multi-stage, multi-application payloads. Traditional tools do a good job screening out the noise of known malware, legacy attacks and blacklisted URLs. They also enforce regulatory and governance policies for appropriate use of applications and resources, including the Internet. However, these tools primarily detect known threats. They must be augmented with dynamic, real-time analysis that detects breaking, unknown threats.

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 personalized phishing emails send a carefully selected target a carefully researched, plausible-looking message and malicious attachment. Or tweets and social media posts include a shortened URL. Each time a victim visits the URL or opens the attachment, a rich payload installs on his computer.

This code often includes exploits for multiple unknown plug-in, browser, application and OS vulnerabilities to ensure it gains a foothold on the system. "Internet Explorer 6 on Windows XP? I have an exploit for that."

How does advanced malware 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 antivirus 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.
- **Antivirus & Web malware filtering:** Since the malware and the vulnerability it exploits are unknown (zero-day), and the Website has a clean reputation, traditional antivirus 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 antivirus 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.[13]

Malicious code can also be carried in on laptops or USB devices, infecting a machine and spreading within 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 antivirus 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.[14] 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 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.

Separate Acts vs. The Entire Show

While these solutions improve every year, they share a fundamental problem. They witness separate acts in the cybercrime performance. One scans email, one inspects exploits, another does file scanning for malware, another looks at URL blacklists. No single tool pulls it all together to watch the whole show: inspect multiple activities, find the common thread and understand the complete series of inbound and outbound communications that represents the entire attack.

Plugging The Security Hole

These shortcomings explain the success of a new category of threat prevention tools adapted to the resilient, evasive and complex nature of next-generation threats. This new generation of security systems complements traditional defenses by detecting and blocking the advanced malware, zero-day and targeted APT attacks that firewalls, IPS, antivirus and Web gateways cannot stop. By combining signatures to rule out the known, dynamic code execution to detect the unknown and real-time inbound and outbound protections, the next generation of security plugs the network hole left wide open in virtually every organization today.

The world leader in fighting next-generation threats is FireEye. Companies around the world in virtually every industry have turned to FireEye to see the full picture of Internet activities, block callbacks that exfiltrate data and derail the communications of advanced persistent threats.

Operating inline or out of band, FireEye malware prevention appliances perform automated, real-time analysis of software behavior. Anything that looks suspicious is executed in an instrumented enviroment where the system monitors activities from active memory up the stack to browser plug-ins. This full-fledged testing can confirm irrefutably the intention 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 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 and email 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.[15]

Next Generation Security for Next Generation Threats

Well-funded cyber criminals have adjusted their techniques from generic, opportunistic and scattershot to targeted, resilient and evasive. Enterprises of all sizes must reinforce their traditional defenses with next-generation threat prevention that understands the nature and intent of these malicious, zero-day and targeted attacks, especially those bearing the hallmark of the advanced persistent threat.

Use FireEye's evaluation program to see the threats your current protections are missing.

About FireEye, Inc.

FireEye is the leading provider of next-generation threat protection focused on combating advanced malware, zero-day and targeted APT attacks. FireEye's solutions supplement security defenses such as next generation and traditional Firewalls, IPS, AV and Web gateways, which can't stop advanced malware. These technologies leave significant security holes in the majority of corporate networks. FireEye's Malware Protection Systems feature both inbound and outbound protection and a signature-less analysis engine that utilizes the most sophisticated virtual execution engine in the world to stop advanced threats that attack over Web and email. Our customers include enterprises and mid-sized companies across every industry as well as Federal agencies. Based in Milpitas, California, FireEye is backed by premier financial partners.

[1] Over 95% of companies evaluating FireEye uncovered compromised hosts in their networks.

[2] 2011 CyberSecurity Watch Survey, US Secret Service, CSO Magazine, Carnegie Mellon, Deloitte: http://www.cert.org/archive/pdf/CyberSecuritySurvey2011.pdf

[3] Source: http://www.syneto.net/images/stories/pdf/commtouch_trend_report_april_2011.pdf

[4] http://www.pcworld.com/businesscenter/article/224898/epsilon_a_watershed_for_an_industry_under_siege.html

[5] http://www.rsa.com/node.aspx?id=3872

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

[7] "The hackers break in on a non-important system, which is very common in hacking situations, and leveraged (sic) lateral movement to get onto systems of interest over time." Greg Hoglund, http://krebsonsecurity.com/2011/02/hbgary-federal-hacked-by-anonymous/

[8] http://krebsonsecurity.com/category/smallbizvictims/

[9] http://www.shadowserver.org/wiki/pmwiki.php/Stats/BotCountYearly shows increase from 25,000 bots to 180,000 bots in 12 months.

[10] http://www.informationweek.com/news/smb/security/showArticle.jhtml?articleID=229000910

[11] InformationWeek's 2010 Strategic Survey

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

[13] Source: Symantec, 2010

[14] 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

[15] In 2010, the cost of a data breach averaged $7.2 million; http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher

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