

Why Next-Generation Firewalls Don't Stop Advanced Malware and Targeted APT Attacks

Executive Summary

Around the world, organizations are investing massive amounts of their budgets in security: over \$20 billion in 2010, and over \$5 billion on firewalls alone¹. However, in spite of the billions invested, 99% of enterprises have malicious infections bypass traditional security mechanisms and compromise the network. Further, 80% experience more than a hundred new infections each week².

Why are organizations so vulnerable despite of all the security investments that have been made? Today, organizations are being hit by a new breed of attack, and the traditional security technologies that have been deployed to date—including firewalls, intrusion prevention systems (IPS), antivirus and Web gateways—have proven incapable of stopping them.

The same holds true for next-generation firewalls (NGFWs). Compared to traditional firewalls, NGFWs typically take a more application-centric approach to traffic classification. Some NGFW vendors have classified approximately 1,300 applications, enabling organizations to inspect traffic flow, irrespective of port or protocol used. This enables security managers to fine-tune the policy controls that govern acceptable use, but does it detect and block the new breed of advanced attacks such as zero-day, targeted attacks or advanced persistent threat (APT) attacks? Not even close.

With more than 286 million new malware variants surfacing in 2010 alone³, it is no wonder NGFWs, like traditional firewalls, fall short when it comes to next-generation threats. NGFWs still rely on third-party vendors to provide traditional antivirus and IPS signatures, reputation analysis, and URL blacklists—approaches that have proven incapable of stopping advanced threats.

This paper offers an overview of the characteristics of next-generation threats, and it details why NGFWs are ill equipped to repel these attacks. Finally, the paper looks at the key capabilities organizations need to effectively thwart next-generation threats.

“NGFWs still rely on third-party vendors to provide traditional antivirus and IPS signatures, reputation analysis, and URL blacklists—approaches that have proven incapable of stopping advanced threats.”

The Characteristics of Next-Generation Threats

Today, the attacks enterprises face, and the criminals behind those attacks, bear very little resemblance to those of just a few years ago. As opposed to known threats, such as well-known malware or spam, today's attacks are dynamic, targeted, and stealthy—consistently evading the traditional security defenses of just about every organization. Following are some of the key characteristics of next-generation threats:

- **Automatically and quickly evolving.** Given the tools now at criminals' disposal, malware and malicious domains are growing increasingly dynamic. Today, 90% of both malicious binaries and malicious domains are changing within hours, and 94% change each day—figures that increased substantially during the first six months of 2011⁴.

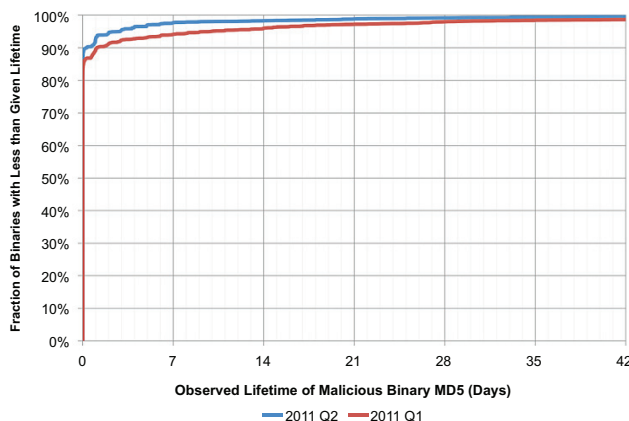


Figure 1: Cumulative distribution function for the period over which we observe a particular binary that is the exact sequence of bytes as captured by the MD5 signature.

- **Built with sophisticated development tools.** Criminals are now leveraging commercial-grade toolkits. These programs enable criminals to use point-and-click interfaces to obfuscate malicious code, which makes it fast and easy to generate a nearly infinite number of malware variants that can effectively bypass traditional security mechanisms. The power of these more sophisticated toolkits is matched by their popularity among criminals: the most widely used 50 malware families are responsible for 80% of all the malware being distributed⁵.
- **Use Web and Email to exploit unknown vulnerabilities.** Modern attacks use the Web and email communication channels to target known, unpatched vulnerabilities as well as unknown, or “zero-day” vulnerabilities in plug-ins, browsers, applications, and OSs.
- **Employ APT tactics.** Today's attacks leverage techniques like camouflage, multi-stage packaging, and targeting to duck traditional defenses and find vulnerable systems and sensitive data.

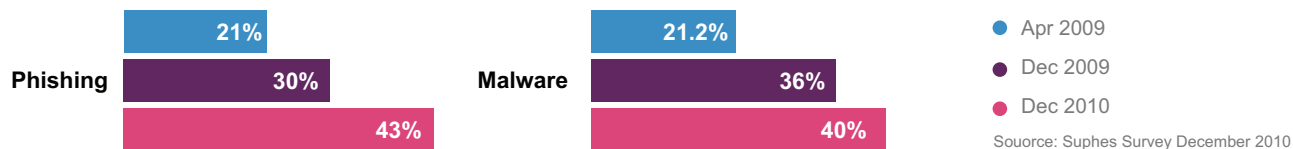


Figure 2: Phishing and Malware reports have doubled from 2 years ago

Why NGFWs Fall Short

Reliance on Signatures

NGFWs do not offer the dynamic protections needed to detect next-generation threats. NGFWs scan the network traffic of supported applications in a single, stream-based scan. Since they integrate antivirus and IPS, NGFWs use signatures, relying on known attacks for their analysis. Quite simply, if the NGFW doesn't have a signature for an attack, it won't detect the attack.

Reliance on URL Black Lists and Reputation Lists

With 94% of malicious binaries and URLs changing every day, the rapidly shifting, dynamic nature of attacks makes it virtually impossible for NGFWs, and the URL black lists and reputation lists that they rely on, to keep pace. By moving their malware to an unknown site (often a compromised server or zombie), and using other tactics, such as short URLs and cross-site scripting, criminals can stay ahead of these list-based defenses. Consequently, malware goes undetected by the NGFW. Further, given the fluidity of next-generation malware, these list-based approaches can actually backfire, generating more false negatives (when a given exploit isn't recognized) and false positives (if a domain is misclassified in the black list).

Lacking Email Security

Spear phishing refers to fraudulent emails targeting a specific individual or organization, typically seeking access to confidential data or credentials. Today, spear phishing represents one of the most common ways APT attacks are initiated. The RSA breach, first reported in March 2011, is one of the more recent and prominent examples in which spear phishing was the first step in a coordinated series of attacks. Because they lack email security controls, NGFWs are ill equipped to stop spear phishing and other email-based attacks.

Self-admitted By Augmenting NGFW With Flawed Cloud-based Analysis

Without any real-time analysis within the locally deployed firewall, NGFWs are unable to address advanced malware and targeted APT attacks. Some are announcing cloud-based analysis to augment the admittedly inadequate in-box NGFW security. This too is fundamentally flawed. Beyond the privacy concerns of sending corporate binaries to a 3rd party, the architectural flaws include the fact targeted APT attacks using email spear phishing would entirely bypass a firewall-initiated cloud analysis. Also, some of the most common exploit tactics, such as Flash® or malicious JavaScript snippets, cannot be analyzed in the cloud outside of the complete Web session flow (even if it were possible for the firewall to carve out those Web objects.) Finally, common file formats and encoded files are also not analyzed.

“Quite simply, if the NGFW doesn't have a signature for an attack, it won't detect the attack.”

Key Requirements for Next-Generation Threat Protection

Today, organizations need a new generation of security system, one that detects and blocks the advanced malware, zero-day, and targeted APT attacks that NGFWs and other traditional security mechanisms miss.

Next-generation threat protection must have signature-less technology to detect the attacks that rely on unknown vulnerabilities, and they need real-time inbound and outbound protections to stop known attacks and data exfiltration attempts. In addition, Web and email have to be monitored to see the full picture of Internet activities, block callbacks that exfiltrate data, and derail the multi-phased communications of APT tactics. Following are more details on the requirements for effective next-generation threat protection.

Deliver Signature-less, Dynamic Security that Thwarts Zero-Day Attacks

To be effective, anti-malware solutions need to provide dynamic, real-time analysis of network traffic and processes, rather than just comparing bits of code to signatures. This signature-less analysis is critical to enabling a product to detect and stop polymorphic malware on the wire as well as malware hosted on dynamic, fast-changing domains.

If suspicious code is detected, it should be executed in an instrumented environment, one in which activities are monitored at every layer in the technology stack, from active memory to browser plug-ins. This full-fledged testing can irrefutably determine the intention and activities of the attacker, zeroing in on real threats and avoiding false positives and false negatives.

Guard Against Malicious Code Installs and Block Callbacks

To be effective at combatting next-generation threats, systems must identify whether malware binaries and executables are malicious. Further, resulting callback communications need to be inspected to detect if they are malicious in nature. This must include monitoring outbound host communications over multiple protocols in real-time to determine if the communications indicate an infected system is on the network. Callbacks need to be identified as malicious based on the unique characteristics of the communication protocols employed, rather than just the destination IP or domain name.

Once malicious code is flagged, its communication ports, IP addresses, and protocols must be blocked in order to completely halt any dangerous transmissions. When the binary of zero-day malware has been captured, the system needs to gather and disseminate the information organizations need to block subsequent attacks using that binary.

“Next-generation threat protection must have signature-less technology to detect the attacks that rely on unknown vulnerabilities, and they need real-time inbound and outbound protections to stop known attacks and data exfiltration attempts.”

Offer a Cohesive View of Protocols and Threat Vectors—including Web and Email

To effectively combat next-generation threats, organizations need systems that have the intelligence to assess threats across vectors, including Web and email. This requires real-time analysis of URLs, email attachments, binaries transiting over multiple protocols, and Web objects to determine whether they're malicious. This is a critical requirement for guarding against spear phishing and other email-based attacks. In addition, the threat information gathered through this inspection needs to be correlated to effectively uncover the nature of the attack, the malware utilized, and any targets that received similar emails.

“To effectively combat next-generation threats, organizations need systems that have the intelligence to assess threats across vectors, including Web and email.”

Further, to effectively defend corporate networks, organizations need systems that inspect across many protocols and throughout the protocol stack, including the network layer, operating systems, applications, browsers, and plug-ins like Flash.

Yield Timely, Actionable Malware Intelligence and Threat Forensics

Once malicious code has been analyzed in detail, the information gathered needs to be fully leveraged. This information should be used for a number of purposes:

- Analysts can use the fingerprint of the malicious code 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.
- Information can be shared through unified intelligence systems that keep other experts and organizations current.

Conclusion

NGFWs deliver improvements over many legacy firewall products. However, firewalls, old and new, are fundamentally designed to enforce acceptable use policies around known ports, protocols, and applications. They offer no real protection against dynamic attacks that cut across communication channels to break into the network. So, by relying on signatures and backward-looking black lists—they are still poorly equipped to contend with advanced malware, zero-day, and targeted APT attacks. To thwart the advanced attacks that are successfully penetrating their defenses, organizations need next-generation threat protection that is signature-less with dynamic code execution to detect the unknown.

- ¹ "Forecast: Enterprise Security Infrastructure, Worldwide, 2008-2014, 1Q11 Update", Gartner, January 2011. <http://www.gartner.com/DisplayDocument?id=1525119>
- ² "FireEye Advanced Threat Report—1H 2011", FireEye, August 2011, http://www.fireeye.com/resources/pdfs/FireEye_Advanced_Threat_Report_1H2011.pdf
- ³ "Symantec Threat Report", Vol. 16, Symantec, April 2011. http://www.symantec.com/content/en/us/about/media/pdfs/symc_2011_ISTR16_the_year_in_numbers.pdf
- ⁴ "FireEye Advanced Threat Report—1H 2011", FireEye, August 2011. http://www.fireeye.com/resources/pdfs/FireEye_Advanced_Threat_Report_1H2011.pdf.
- ⁵ "FireEye Advanced Threat Report—1H 2011", FireEye, August 2011. http://www.fireeye.com/resources/pdfs/FireEye_Advanced_Threat_Report_1H2011.pdf.

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 traditional and NGFWs, IPS, antivirus 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.