FireEye™

White Paper

5 Design Principles for Advanced Malware Protection

Winning the war against next-generation threats

Table of Contents

FireEye™

White Paper

Executive Summary

In a 2010 poll of chief information security officers and senior IT security directors at Fortune 500 corporations, all respondents stated that they consider malware, whether viruses, Trojans, bots, or other advanced persistent threats, to be a serious threat to their enterprise IT security. A 2011 Ponemon Institute study found that the average 2010 per-incident data breach cost was $7.2 million.[1] Advanced malware continues to place organizational data and network resources at increasing risk, with break-ins at RSA Security and Epsilon marketing and the continuing success of Zeus demonstrating the range of targets for these cyber weapons.

The state of IT security has reached this point because traditional defensive technologies have stagnated in the face of a fast-evolving offensive threat. With a strong profit motive and at times nation-state objectives, cyber criminals have aggressively enhanced and upgraded their malware. By working across multiple protocols and on multiple fronts, from unknown OS and application vulnerabilities to social engineering, malware works its way through traditional defensive layers. Victims span all industries from the largest defense contractors and global financial institutions to regional grocery store chains and healthcare networks.

As a result, IT security teams are left with a devil's bargain. They could tightly restrict the use of the Web to limit user access to today's primary threat vector, Web 2.0 applications. However, this often creates the unacceptable costs of business disruption, user dissatisfaction and false positive triage when signature and heuristic rule sets are too aggressively deployed. The alternative has been to implement industry "best practices" using a layered defense, but with easy-to-bypass technologies like rules-based firewalls, signature-based antivirus and intrusion prevention, or list-based URL filters.

This paper offers a better and more current framework to understand both the next-generation threat landscape of advanced malware and the five key design principles needed to eliminate the devil's bargain implicit in today's dated and highly ineffective rule-, signature- and list-based defenses.

Advanced Malware Defined

Malware innovations have been driven by attackers' quests to gain increasing control of compromised computer systems and the networks in which they reside. Whether attackers use viruses, Trojans, bots or rootkits, today's malware is designed for the long-term control of compromised machines. Often offensive tactics disrupt client-based security, like re-writing the Windows HOSTS file to disrupt antivirus signature and patch updates, or resetting Microsoft security updates to manual. Advanced malware also establishes outbound communications across several different protocols to upload stolen data and to download instructions and further malware payloads for other reconnaissance and malicious purposes.

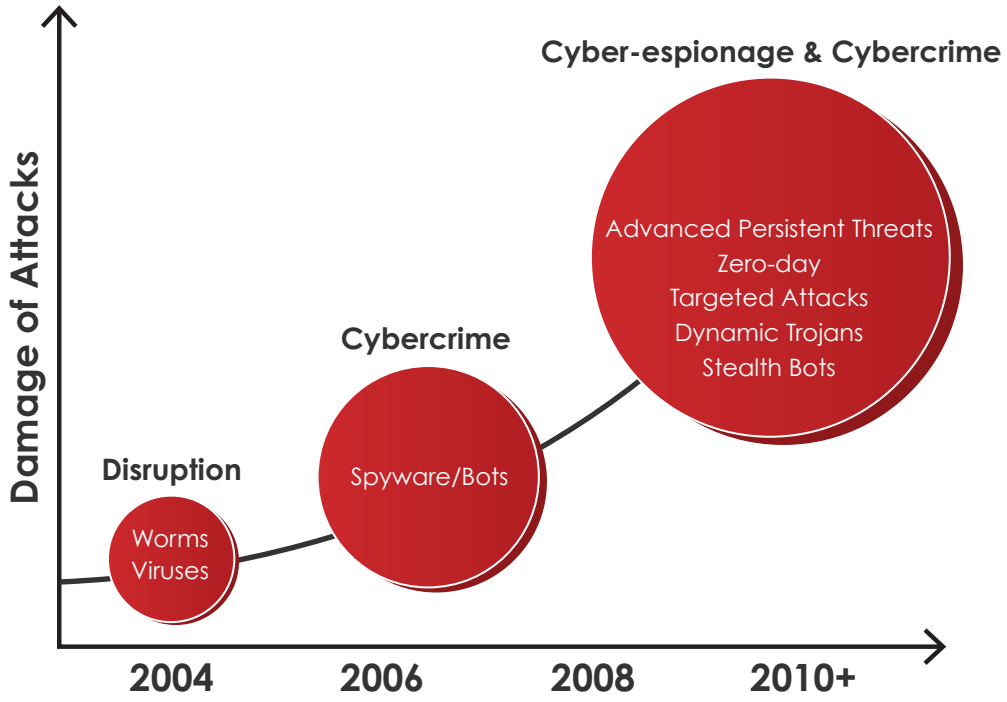
Early cyber attackers compromised systems primarily for fame and bragging rights. As criminals became aware of the value of information being placed online, they quickly became involved in developing

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

Security teams are faced with a devil's bargain: restrict access, disrupt business or implement ineffective defenses.

malware for profit. Law enforcement, computer crime experts and the military are now playing catch up to the threat posed to consumers, businesses and national security as cyber criminals cash in on stolen identity data, fraudulent online transactions and cyber espionage. It is clear that criminals with profit motives or political agendas are the main cause for the explosion of malware as we know it.

Web sites and applications now support user-contributed content, syndicated content, iFrames, third-party widgets (or applets) and convoluted advertising distribution networks into which malware can easily be injected. The malware that criminals have developed is dynamic and stealthy. It leverages unknown vulnerabilities across a range of applications and communications protocols. The specific characteristics of particular strains of malware differ depending on the purpose of the attackers, be it for cyber crime, cyber espionage or emerging cyber warfare scenarios.



As professional criminals have moved in, malware has grown much more sophisticated

Cyber criminals have developed ways to bypass outdated security techniques, such as signatures, leaving businesses and consumers vulnerable to attack. Signature-based technologies like IPS and antivirus software, both within perimeter and endpoint solutions, are increasingly ineffective against this rapidly evolving, blended threat, as is evidenced by the continued and successful intrusions into commercial, federal and educational networks. At the same time, more and more businesses and consumers are storing data on the network, "in the cloud," and conducting transactions through the Internet, making cyber crime more attractive than ever.

Malware innovations have been driven by attackers' quests to gain increasing control of compromised computer systems and the networks in which they reside.

Understanding Next-Generation Threats

An advanced malware attack can no longer be seen as a single incident consisting of exploit, infection and remediation stages. Today's attacks are coordinated efforts to penetrate an organization's defenses and establish a foothold for the purposes of reconnaissance, network asset exploitation, data exfiltration, data alteration, data destruction and ongoing surveillance.

On January 12, 2010, Google disclosed it was one of more than 20 companies successfully targeted by a coordinated effort to gain access to sensitive systems and confidential information. Known targets spanned a variety of industries, including the financial, technology and chemical sectors. These attacks later became known as "Operation Aurora" and are a very useful example of what advanced attacks and malware actually look like—and how commonly used security technologies failed to combat these advanced, persistent threats.

The Aurora attacks leveraged an unknown, zero-day Internet Explorer 6 vulnerability to compromise systems within these targeted corporations. Attackers then installed a Trojan that would communicate back to a criminal command and control server with the capability to send and receive a variety of different commands and subsequent malware payloads. These subsequent malware tools enabled attackers to gather intelligence about the compromised network with the aim of locating and exfiltrating confidential data.

Advanced malware is part of advanced, persistent cyber threats that act in a coordinated fashion to penetrate an organization's defenses and establish a long-term foothold in the network.

The first step of an infection is the initial exploit or social engineering attack. It leads directly to a series of follow-on malware infections that persist despite repeated attempts to scan and disable the attack. As malware has become more sophisticated, conventional client-based antivirus scans and network-based intrusion scans no longer are able to disrupt and stop these coordinated sets of infections and attacks. While some infections are detected and removed by scans, the criminal maintains control over the system. Other, often zero-day, malware components that were not removed allow him to re-install malware and disrupt endpoint security to prevent future removal.

Advanced Malware in Action

Cyber Crime

When it comes to cyber crime, the criminal's main goal is to steal assets, services or financial information that can eventually be turned into hard currency. There are attackers who are making money by infecting and linking up thousands of computers, often referred to as "botnets." These are then monetized in a variety of ways. For example, some criminal organizations rent out the computing power of these networks to send phishing spam. In other cases, criminals perpetrate extortion schemes by threatening to take a business's website down through distributed denial of service attacks. They have even jumped onto the Cloud Computing trend with "Malware-as-a-Service" offerings, where cyber criminals sell capacity and services on a subscription basis to each other. [2]

[2] *Fest, Glen, "Malware-as-a-service Takes a Bow," Bank Technology News. http://www.americanbanker.com/btn_issues/21_5/-352304-1.html*

Increasingly, cyber criminals are focused on stealing financial and personal information that can be directly monetized. Criminals recently targeted RSA to get access to intellectual property for their two-factor authentication (SecurID) implementation.[3] Epsilon marketing provided access to email account information with business relationship details that could be used to allow phishing attacks to get past spam filters.[4]

The rampant Zeus Trojan, or Zbot, steals users' online banking credentials. It does this by hijacking an online banking session and re-writing Web pages on the victim's PC to look like the bank's website. This spoof tricks users into typing in their banking credentials, which the Zeus Trojan then uploads to a criminal server to be aggregated and sold to the highest bidder.

In response, financial institutions have increased layers of security around authentication and identity verification, including two-factor authentication for bank transactions. Virtually overnight, however, malware has evolved to circumvent these new safeguards. "Online thieves have adapted to this additional security by creating special programs—real-time Trojan horses—that can issue transactions to a bank while the account holder is online, turning the one-time password into a weak link in the financial security chain."[5]

Cyber Espionage

Cyber espionage uses advanced malware to covertly obtain data that is considered secret or confidential. In January, 2010, it was reported that, "at least three US oil companies were the target of a series of previously undisclosed cyber attacks that may have originated in China and that experts say highlight a new level of sophistication in the growing global war of Internet espionage."[6] As more information is moved online, we will only see a continued increase in the use and sophistication of cyber espionage.

Given the relatively low barriers to entry, superior cyber espionage capabilities will not be the exclusive domain of traditional super powers. No doubt, the efforts of much of the global intelligence community are focused on cyber espionage. There have been a few public cases of advanced malware being used in corporate espionage, including Operation Aurora and the aforementioned attack targeting the oil industry. In both cases, malware that was stealthy and unknown to signature-based systems was highly effective in stealing sensitive information.

Cyber Warfare

Emerging cyber warfare scenarios would most likely involve using sophisticated and stealthy malware in reconnaissance activities, intelligence gathering, communications disruptions, and critical infrastructure attacks. Sophisticated technical capabilities, including hacking, have had limited usage within conventional warfare scenarios thus far, not yet in a coordinated and targeted attack against a country's communication and critical infrastructure. Known cyber reconnaissance infiltrations have taken place, and in part led to the establishment of the US Cyber Command in September 2009. Other Cyber Command operations around the world have now also been established, so it is clear that cyber warfare is a distinct possibility with all sides considering their options and preparing defenses.

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

4 *http://garwarner.blogspot.com/2011/04/epsilon-phishing-model.html*

5 *Lemos, Robert. "Real-Time Hackers Foil Two-Factor Security." MIT Technology Review, September 18, 2009. http://www.technologyreview.com/computing/23488/?a=f*

6 *Clayton, Mark. "US oil industry hit by cyber attacks: Was China involved?" Christian Science Monitor, January 25, 2010. http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved*

Disrupting Next-Generation Threats

Given the serious consequences and ineffectiveness of current solutions, FireEye is publishing and sharing its five key principles to designing an effective network-based defense. Solutions should be held up to these criteria as part of any investment decision involving malware defenses. The 5 key principles are:

1. Dynamic defenses to stop targeted, zero-day attacks
2. Real-time protection to block data exfiltration attempts
3. Integrated inbound and outbound filtering across protocols
4. Accurate, low false positive rates
5. Global intelligence on advanced threats to protect the local network

Dynamic Defenses to Stop Targeted, Zero-day Attacks

To be effective, anti-malware solutions need to be intelligent enough to analyze network traffic and processes, rather than just comparing bits of code to signatures. Advanced malware has been developed with traditional defenses and software architectures in mind to maximize its chance to exploit an end-user system.

Dynamic analysis, as opposed to static signature-based comparisons, is critical to enable a product to detect and stop polymorphic malware on the wire as well as malware hosted on dynamic, fast-changing domains.

In order to address these advanced threats, real-time, dynamic, and accurate analysis is critical. Rather than relying on signatures and lists, we must be able to dynamically recognize new attacks in real time, without requiring a priori knowledge of vulnerability, exploit or variant, and then prevent system compromise and data theft.

Real-time Protection to Stop Data Exfiltration Attempts

To protect the network, real-time analysis and blocking are essential to stopping data exfiltration that can take place within minutes, if not seconds, of the zero-day infection. It is important to be able to dynamically analyze network traffic to capture and detect zero-day malware, but equally important to provide real-time capabilities to stop the outbound callback communications to disrupt the attack and halt the flow of data.

Integrated Inbound and Outbound Filtering Across Multiple Protocols

Advanced threats include attacks on multiple fronts, exploiting the inability of conventional network protection mechanisms to provide a unified defense. As soon as one vulnerability is defended, network attacks quickly shift to another.

It is now possible to have both inbound attack detection and outbound malware transmission filtering in a single appliance form factor. Administrators gain a clientless solution that is easy to deploy and maintain. This integrated solution allows coverage across the many vectors used in attacks and can keep pace with the dynamic nature of attacks. Defending corporate networks from the advanced malware in next-generation threats requires new protections that function across many protocols and throughout the protocol stack, including the network layer, operating systems, applications, browsers and plug-ins like Flash.

An integrated approach enables the most comprehensive threat protection against malware that attacks across multiple vectors to penetrate the network. The initial compromise of a system could be a social engineering attack like a spear phish email with a URL or malicious PDF. Once the dropper malware is installed, it calls back out to upload stolen data and download further malware payloads. With both inbound and outbound threat protection, it is possible to protect against next-generation threats and go beyond simple signature matching or rudimentary packet analysis.

Accurate, Low False Positive Rates

Other technologies, whether heuristic or behavioral analyses, are touted as an encouraging development, but in practice they are too inaccurate or compute intensive to function as standalone, real-time security mechanisms. This methodology often augments an anti-malware solution's signature protections, but at the same time increases the likelihood of false positive alerts.

The sheer volume and escalating danger of advanced malware attacks are overwhelming limited IT resources and outmaneuvering conventional defenses. For most enterprises, traditional network connection-oriented and software-based defenses are inadequate, because of the gaps they leave in security coverage. However, trying to integrate conventional defenses from multiple vendors is far too complicated and costly an undertaking for an enterprise IT group.

Global Intelligence on Advanced Threats to Protect the Local Network

For preemptive protection against a dynamic cyber threat, it is important to have a global network to provide the latest intelligence on malware threats and zero-day attacks. Real-time malware intelligence can protect the local network against zero-day malware and advanced persistent threats. It can stop outbound callbacks that threaten to exfiltrate sensitive data. By building an intelligence-sharing network with customers, technology partner networks, and service providers around the world it is possible to share and efficiently distribute malware security intelligence to essentially serve as an Internet cyber crime watch system and stop both inbound attacks and unauthorized outbound callbacks and prevent data exfiltration, alteration, and destruction.

FireEye Malware Protection Systems

FireEye offers next-generation protection against stealth malware to prevent data loss and intellectual property theft. The FireEye Web and Email Malware Protection Systems (MPS) stop zero-day attacks and outbound callbacks while inoculating networks from future attacks. They stand behind existing firewalls, IPS, AV and Web gateways to block attacks that have sneaked past.

To stop zero-day attacks, FireEye MPS appliances use a Virtual Execution (VX) engine and Callback Filter to detect inbound unknown malware, stop its outbound callback transmissions and distribute dynamically generated malware intelligence to protect against future attacks. With the FireEye Malware Protection Cloud, customers receive global security intelligence to protect their local network. FireEye eliminates the headache of false positives and tuning associated with traditional defenses. By blocking the 90% of malware that conventional defenses miss and working at extremely low false positive rates, FireEye delivers a rapid security ROI.

FireEye is able to accurately block unknown threats using the VX engine, a full-featured virtual test environment that executes suspicious code in a multi-stage detection engine including operating systems, applications, browsers, and plug-ins. It captures details about the attack that allow FireEye to fingerprint confirmed malware and block outbound malware callbacks across multiple protocols, including HTTP, IRC, FTP and other protocols designed by cyber criminals.

- **Virtual Execution Engine:** Inbound identification and blocking of stealth malware attacks using aggressive heuristic capture coupled with virtual machine confirmation of attacks
- **Callback Filter:** Outbound tracking and blocking across protocols of unauthorized communications to criminal servers

FireEye appliances deploy within the network security layer to complement existing network and endpoint security solutions by blocking unknown threats and their outbound communications and feeding critical and timely security intelligence to the IT organization. Endpoint security software, for example, still serves a critical role within IT security since it protects against legacy infections and provides cleanup services. Next-generation firewalls can overlay beneficial policies to manage user- and application-based use of the Internet.

The primary challenges today are zero-day threat and APT attack detection and outbound blocking of malware callbacks. IT needs tools like FireEye in order to mitigate the risk of massive data losses, while providing critical attack insight to assist IT security analysis and response processes.

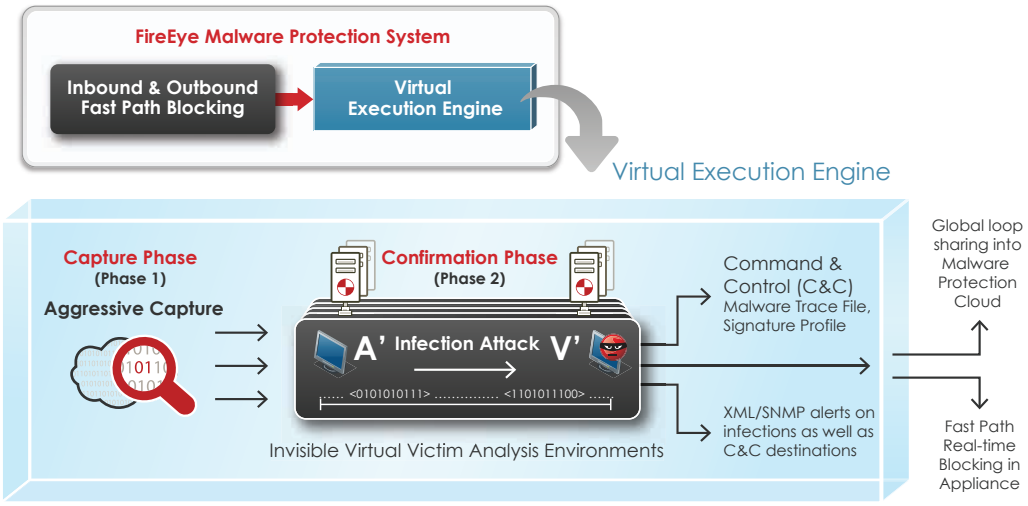
Virtual Execution Engine: Beyond Signatures

FireEye has pioneered the use of transparent virtual victim machines operating in a network appliance to detect new attacks and to analyze malware infections in real time. The Virtual Execution Engine consists of a first phase analysis to capture suspicious Web objects, emails and executables using aggressive heuristics. After casting a wide net for malware, a second phase is employed to eliminate false positives. FireEye's proprietary virtual machine analysis technology acts as a second phase filter to confirm infections and remove any false positives.

Phase 1—FireEye network appliances capture suspicious traffic based on complex heuristics

Phase 2—To eliminate false positives, suspicious Web traffic is replayed within proprietary virtual machines to clearly identify malware, both known and zero-day

With zero-day malware confirmed in the virtual environment, additional malware characteristics are captured during the analysis, such as callback destinations, binary analysis, registry changes and other file corruptions. The analysis is then fed into the 'local loop' where outbound communications by this malware are terminated, and future inbound attacks are blocked. The malware fingerprint can also be shared to the FireEye Malware Protection Cloud, thereby protecting others immediately against emerging malware.



FireEye technology works inbound and outbound to block multi-phase attacks

Callback Filter: Outbound Callback Protection

By tracking unauthorized, outbound communications to criminal C&C servers, PCs infected with stealth malware can be flagged for cleanup and data exfiltration attempts blocked. To ensure accurate detections and account for "dual-purpose" Web servers (that host legitimate sites as well as the malicious site), FireEye also analyzes the protocols and content used to communicate to those criminal C&C servers. Using fully qualified outbound callbacks, FireEye can accurately detect infected machines on the corporate network and block their outbound data theft attempts.

FireEye Malware Protection Cloud: Global Sharing to Secure the Local Network

Taking this multilayered approach, FireEye has the unique capability to provide real-time malware intelligence gathered by its appliances to its customers worldwide via the FireEye Malware Protection Cloud. Every device can be kept up-to-date on the latest criminal C&C servers to identify infected machines as well as the latest in malware attack tactics. FireEye offers a fundamentally new technology to defend against zero-day, targeted attacks, bots, Trojans and advanced, persistent threats. FireEye security appliances can accurately block attacks that use techniques like polymorphism and obfuscation to exploit client browsers and operating systems.

Next-Generation Security for Next-Generation Threats

The use of sophisticated malware has been accelerating at an extraordinary pace, primarily due to economic incentives and political motives. By infecting systems with multiple types of malware, cyber criminals are able to maintain long-term control over a compromised PC system. In order to break this stranglehold, any proposed solution must support several key principles. The ability to detect zero-day, unknown malware is necessary, but not sufficient. Blocking outbound callbacks is necessary, but not sufficient. The solution must integrate inbound and outbound blocking to stop the data exfiltration, which is the primary objective of today's malware infections. High accuracy is required to avoid the clutter of false positives, and constant updates help maintain defenses against fast-paced threats.

FireEye solutions include protection across inbound and outbound paths to combat advanced malware, zero-day and targeted APT attacks. Use our free network threat evaluation to uncover next-generation threats hiding in your network. Over 95% of companies discover compromised hosts. Most see such strong ROI they purchase their evaluation gear.

Drop an evaluation system in behind your gateways and see what your current security is 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.

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