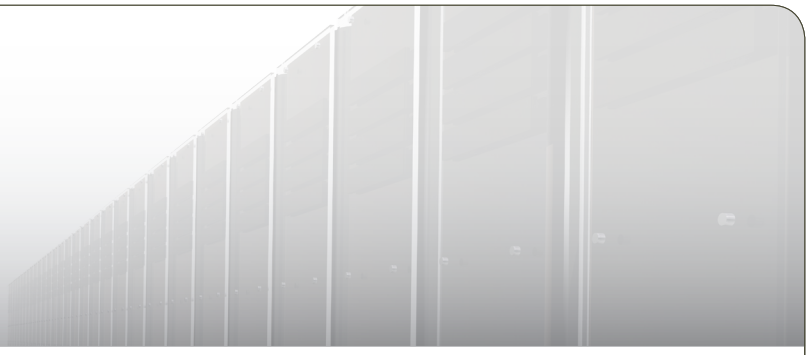


Protecting Data From the Cyber Theft Pandemic

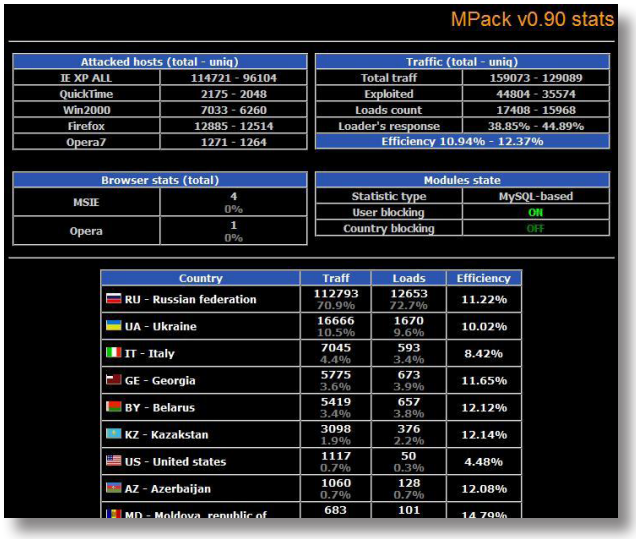
A FireEye Whitepaper - April, 2009

Table of Contents

Executive Summary

Malware-related data breaches have reached pandemic proportions as criminals discover that Internet crime is easy to commit, highly lucrative, and largely under-policed. With a few hundred dollars, a cyber criminal can begin a career of breaking into computers to steal identity and confidential data for sale to the highest bidder. Fraudsters who purchase the data have developed a variety of schemes to monetize that information ranging from transacting unauthorized stock trades to transferring funds to offshore bank accounts. The cyber crime economy is so robust that there is a vibrant market for professional malware toolkits available for $500 to $1,000 and come pre-configured with a range of attack modules, exploit 'maintenance' updates, and 24 x 7 online technical support.

This white paper will cover current and emerging trends of stealth malware, such as moving primarily to the Web since most organizations allow Web traffic into the network. It will also cover new advances in network security technologies that use multi-phase heuristic and virtual machine analysis to detect and mitigate the damages that result from malware-related data thefts.



MPack, a PHP-based malware kit, was released in Dec. 2006

Today's Insider Threat Is Stealth Malware

Law enforcement, computer crime experts, and even the military are 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 no surprise that the rise in cyber crime has coincided with the increased use of the Internet and especially "Web 2.0" technologies. Web sites and applications now support user-contributed content, syndicated content, iframes, third-party widgets (or applets), and convoluted advertising distribution networks into which 'stealth' malware can easily be injected somewhere along the line. In a 2007 USENIX paper, Google researchers determined that approximately 9% of all suspicious web sites launched "drive-by" downloads of stealth malware binaries.[1] Government studies[2] estimate that 65% of all exploits now enter via the Web and IBM Internet Security Systems (ISS) estimates that nearly 100% of Web attacks now utilize obfuscated JavaScript as a very effective technique to bypass antivirus and intrusion prevention.

Today, once a PC is infected with stealth malware, it typically opens two-way communications to a "command and control" (C&C) server to establish a channel back to the cyber criminal. This allows the "bot" (as in "robot computer") to report status as well as any valuable information that is immediately accessible. Groups of these remotely controlled, malware-infected computers are commonly called botnets, and serve as the foundation of most cybercrime on the Internet.

How do victims get infected? A user may be drawn by a phishing e-mail to a Web site hosted on a hijacked server, which serves up a browser exploit; this downloads and installs a bot on the user's PC. The bot then downloads more malware like "keyloggers" that silently record keyboard and mouse activities to execute further criminal activities,

Recent Research[3] Has Found:

- *11 % of the world's computers are enmeshed in at least one botnet*
- *23 % of home computers become infected despite having security enabled*
- *72 % of corporate networks larger than 100 PC's have an infection*

[1] Niels Provos, Dean McNamee, Panayiotis Mavrommatis, Ke Wang, and Nagendra Modadugu: The Ghost in the Browser Analysis of Web-based Malware, May 2007.
[2] David Barroso, ENISA Position Paper No. 3: Botnets – The Silent Threat, November 2007 , http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_botnets.pdf.
[3] Panda Security, http://www.pandasecurity.com/homeusers/media/press-releases/viewnews?noticia=9077

such as stealing user credentials and capturing other sensitive information. All of this takes place without the knowledge of the user or administrator. As their prevalence has increased, remote-control malware/botnets have become serious concerns for security administrators.

The recent January, 2009 malware-related data thefts at Heartland Payment Systems and earlier malware infiltrations at Hannaford Supermarkets, University of Florida Medical Center, and NASA underscore the escalating threat of malware-related data breaches. The Identity Theft Resource Center, a nonprofit group focused on understanding and preventing identity theft, reported that 656 known security breaches had taken place in 2008, reflecting a 47 percent increase over 2007's total. As of March 17, 2009 the resource center had already reported 110 breaches in 2009.

DNA of an Ideal Solution:

- *Dynamic, real-time detection of threat: Finds the latest stealth, 0-day attacks*
- *Accurate detection: No false positives, and no false negatives*
- *Return on security investment: Easy to install, manage, support and scale*

Stealth Malware Attacks Are Outmaneuvering Conventional Defenses

Defending corporate networks from today's malware-related data thefts requires modern protection that goes beyond current signature- and heuristic-based detection techniques. Modern threats exploit the inability of conventional network protection to provide a unified defense against a criminal who attacks on multiple fronts, from OS and browser vulnerabilities to social engineering. The anachronistic concept of detecting infections with a single technique, such as signatures, has left many businesses and consumers open to attack, despite their deployment of antivirus and IPS (intrusion prevention systems). The sheer volume and escalating danger of modern attacks are overwhelming limited IT resources and outmaneuvering conventional defenses that may already be in place.

To enable a more efficient IT security process, accurate and timely identification of infected machines is the first step in preventing malware-related data breaches. And, the only viable solutions are those that provide thorough coverage across the many vectors that are used in attacks.

An Effective and Efficient Response to Modern Stealth Malware

FireEye offers a modern defense against stealth malware to prevent data loss and intellectual property theft. The multi-stage detection engine unifies virtualization and network security to very accurately identify Web malware and botnets that do not belong in the network. From a high level, there are two core techniques:

- **Inbound detection** of stealth malware attacks using the FireEye Analysis & Control Technology (FACT)
- **Outbound tracking** of unauthorized communications to criminal C&C servers

FireEye appliances deploy within the network security layer to complement existing network and endpoint security solutions by 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 clean-up services. The key is still detecting zero-day infections early to mitigate against massive data losses, while reinforcing IT security response processes.

The FireEye Analysis and Control Technology: 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/botnet infections in real time. The FACT engine consists of a 2-phase analysis to capture suspicious Web traffic using heuristic detection, and then eliminate false positives using the virtual victim machine analysis technology.

Inbound Attack Detection

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

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

Outbound Callback Detection

With an increasingly mobile workforce, there is a substantial risk of off-site infections. By tracking unauthorized, outbound communications to criminal C&C servers, mobile PCs infected with stealth malware can be clearly flagged for clean-up. To ensure accurate detections and account for "dual-purpose" Web servers (that host legitimate sites as well as the malicious site), FireEye also tracks the port and protocols used to communicate to those criminal C&C servers. Using fully qualified outbound callbacks, FireEye can accurately detect previously infected machines on the corporate network.

Global Cooperation to Prevent Data Thefts

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 Analysis and Exchange (MAX) Network. Every device is now kept up-to-date on the latest criminal C&C servers to identify infected machines as well as the latest in stealth malware attack tactics. FireEye offers a fundamentally new technology to defend against zero-day, stealth malware and botnets. FireEye security appliances detect stealth malware that uses techniques like polymorphism and obfuscation to exploit client browsers and operating systems. Blended threats like Web-based malware and botnets now aggressively evade and disrupt legacy security technologies, but cannot escape FireEye analysis. Find out more at our Web site (http://www.fireeye.com) or at our Malware Intelligence Lab blog (http://blog.fireeye.com/).

About the FireEye Solution

The FireEye security appliances and FireEye Malware Analysis & Exchange (MAX) Network service together provide comprehensive anti-malware and anti-botnet protection. FireEye appliances use virtual victim machines to analyze enterprise networks for Web-malware and related bot activities on compromised machines. The FireEye MAX Network is a globally deployed malware discovery and analysis service that provides subscribers with the most current botnet and Web malware intelligence to complement on-premise anti-malware security appliances. It catalogs and disseminates security intelligence such as the inbound attack vector as well as the outbound call-back channels used to steal data. This is all derived from malware analyses which are conducted by interconnected networks of FireEye security appliances selectively deployed at service providers around the world. FireEye's solution offers the industry's first complete global and local anti-malware protection to precisely identify, understand, and stop emerging botnet and Web malware threats.

About FireEye, Inc.

FireEye, Inc. is the leader in anti-malware and anti-botnet protection, enabling organizations to protect critical intellectual property, computing resources, and network infrastructure against Web malware and botnet infiltration. Today's most damaging attacks are perpetrated through Web malware that forms into highly organized botnets, or networks of remotely controlled, compromised machines. FireEye delivers a complete solution that is designed from the ground up to detect and protect organizations from advanced Web malware and botnets through global and local intelligence and analysis. The company is backed by Sequoia Capital, Norwest Venture Partners, JAFCO, SVB Capital, DAG Ventures, and Juniper Networks. For more information, contact (408) 321-6300 or email: info@fireeye.com.

www.fireeye.com

For more information, contact (408) 321-6300 or email: info@fireeye.com.