



BLOCKING MALWARE AND SPYWARE WITHOUT SIGNATURES

JULY 2005



Introduction

Contending with malware – a term that encompasses everything from viruses and worms to spyware and blended-threat attacks – is the most taxing burden on IT staff today. Research firm Computer Economics reports that losses related to malicious code in 2004 rose nearly 40% to over \$17B [worldwide](#). Businesses large and small suffer productivity losses, delays, service outages, damages to brand, theft of business identities and unauthorized disclosures of sensitive and regulated information daily.

A serious problem over the past five years, malicious code attacks have escalated in unprecedented numbers in the past twelve months:

- The [2004 CSI/FBI Computer Crime and Security Survey](#) indicates that, “the virus category emerged for the first time as the incident type generating the largest total losses.” More sobering than this statistic is the fact that “[desktop] antivirus (AV) software was reported as being used by 99 percent of the organizations.
- In its State of Spyware Report, anti-spyware vendor Webroot reports that among the 35,300 systems scanned, representing more than 18,000 companies, nearly 87% had some form of spyware infestation. More disturbing statistics from the report: one in seven PCs in the business world is infected with a keystroke logging program; and the infection rate among certain businesses has reached nearly twelve percent. Webroot also estimates the number of Web sites suspected of hosting spyware near 220,000 worldwide.

While Web sites are increasingly contributing to the spread of malicious code, email continues to serve as its major partner in crime. At this point, email servers more frequently serving as a delivery agent for malicious messages than legitimate mail:

- Message Labs Intelligence Annual Email Security Report indicates that in 2005, one in 16 email messages (6.1%) contained a virus, and that the number of variants of any given virus reported has increased dramatically.
- [Postini](#) reports that 70.1% of the more than 200 billion email messages processed contain spam. Spam figures are fairly consistent across the industry: Message Labs also reports that over 73% of the nearly 12 billion emails processed through its anti-spam gateways contained spam.
- Message Labs also reports that phishing emails increased ten-fold in 2004 from an average of 240,000-400,000 scam emails in the first six months to more than 4 million per month by year end, this figure is also consistent across the industry.

More worrisome than the statistics is the fact that the majority of malicious code today is produced for profit, and delivered with criminal intent. Malicious code development isn't an amateur activity, but a lucratively profitable criminal industry. Ten years ago, your average virus writer developed a worm without pay and exclusively for notoriety or peer respect and recognition. Today, spyware companies pay programmers salaries commensurate with those offered by legitimate businesses. Organized crime sets up shell companies to develop phishing and scam Web sites.¹ As an indicator of how serious the problem is, intelligence agencies investigate any "credible threat" of a terrorist-induced, fast-propagating, highly debilitating worm.

Signature-based Countermeasures: Necessary but Not Sufficient

Many security gateways offer protection against malicious code attacks by building upon the success of anti-malware software commonly installed on end user computers and servers today. Most desktop and server antivirus/anti-spyware software detects and blocks threats by comparing files against known malicious code before it is written to permanent storage.

Thousands of instances of malicious code have been identified, and so for efficiency's sake, anti-malware implementations typically compare hash values (commonly known as 'signatures') of known malware against a hash they compute on an arriving file. Hashes are used because for all practical purposes, a hash, like a human fingerprint, is unique to a given file. If the anti-malware software sees that the hashes are equal, the file is considered malicious code and is blocked.

Gateways that employ signature-based methods extend this model by examining files before they are delivered to client and server machines. This added measure of defense is critical because sophisticated virus strains often attempt to disable desktop AV solutions and other security software. The only place to block malware that behaves like this is at the gateway.

Signatures are an effective and proven way to block known malicious code attacks, as long as signatures are available. However, relying exclusively on signature-based detection has drawbacks. The most obvious is that if you haven't identified a file as containing malicious code, you can't create a signature so you have no "fingerprints" to compare arriving files against. To varying degrees, malware countermeasures compensate for this by applying heuristics.

Some malware detection methods emulate file activity in a controlled space (e.g., sandbox); others inspect suspect files for tell-tale "evil strings" (e.g., subject lines or error messages). These techniques increase detection rates but at the expense of processing and delay and in some cases, increased false positives.

¹ Dennis McCafferty, "Organized Cyber-Crime," Web Host Industry Review, September, 2004

Additionally, signature-based detection typically offers no defense against information leaks, e.g., where an attacker has succeeded in compromising a host on your trusted network and is already uploading spreadsheets and sensitive documents from this machine.

Lastly, when you rely exclusively on signatures at a security gateway, you must examine every file that passes through the system, which puts a heavy toll on gateway processing. Gateways vendors make use of acceleration hardware or ASICs to improve performance. But this strategy again throws organizations into an arms race they ultimately cannot win.

Today's rules of engagement heavily favor the bad guys. Knowing how anti-malware measures work, virus writers modify code and create variants to evade detection: Bagle, Netsky, and MyDoom are all too familiar examples of this practice. Spyware developers in particular, excel at this high-stakes game of cat-and-mouse: the notorious CoolWebSearch spyware already has over seventy known variants. Spammers and phishers employ evasion tactics in email messages as well. Spammers study how heuristics-based anti-spam measures detect spam, and try to defeat them by using character substitution and keyword evasion. Worse, as anti-spam measures improve, spammers simply increase the volume to compensate for reduced delivery success: a success rate of one in one thousand proved [profitable](#) enough to make convicted porn spammer Jeremy D. Jaynes a multi-millionaire.

Relying on signatures as the only or primary line of defense puts an organization in a highly reactive mode and dependent on the ability of vendors to identify new threats, define signatures, and distribute them. [Virus response services](#) backed by service level agreements (SLAs) only commit to a 2-hour response following a virus submission, but the Sapphire Worm (SQL Slammer) infected the majority of vulnerable hosts within ten minutes (see [Analysis of the Sapphire Worm](#)). Comprehensive and Zero Day protection against malicious code attacks requires a more extensive set of security measures.

Back to Basics

To effectively contend with malicious code, organizations must return to basics and consider whether the baseline security policy they enforce is adequate to contend against malicious code. Consider the following two security philosophies:

1. Allow all users unconstrained access to all types of content, and examine every email message, message attachment, and Web page object using signatures to identify and block malicious code. This approach enforces a baseline security policy, "that which is not expressly denied is allowed".
2. Block all but a defined set of data objects you trust to be benign (e.g., attachments and message body types, hyperlinks, etc.); limit access to those provisionally-trusted objects to authenticated users, according to the user's group or role; and then use signatures to identify and block malicious code as an added layer of defense. This approach espouses the security policy, "that which is not expressly allowed is denied."

The second and stronger approach employs a 'multi-layered defense'. The first layer narrows the malware attacker's windows of opportunity by applying user-based authentication and authorization. A single filtering rule on the firewall that prohibits user access to an entire category of content (such as "executables") is defined. This accomplishes more, and with fewer resources, than a signature-scanning malware engine can with a database of even 100,000 signatures of malicious code. Simply put, the new malicious code that will be signature number 100,001 tomorrow is caught if you're blocking users from downloading executables today. Since malware might still slip through in an allowed content type, pattern matching at the gateway is applied against all allowed types as a second line of defense.

Layered defenses are widely accepted and effectively used today. Consider how the overall effectiveness of desktop and server security is improved when antivirus measures on a system are complemented with file anti-tampering measures and stringent security policy administration. Or consider that knowledgeable Web administrators don't rely exclusively on antivirus software for Microsoft® Windows® servers when they configure Internet Information Server for public-facing Internet services. More commonly, savvy administrators will eliminate user accounts on servers; remove unnecessary services; restrict access to critical file systems; and thus layer or harden the server against attacks. Advanced Web administrators will use URL blocking and file system integrity-checking software on the server itself.

Far too many organizations use generously permissive acceptable use policies. Security can be made even more effective when you base your policy upon a principle of least privilege, which essentially says, "Only provide users access to what they need". To implement this:

1. Establish a user's identity
2. Determine if the user is authorized to access this type of data object:
 - o Using this service
 - o From this device
 - o From this location

This approach works equally well for both incoming and outgoing traffic. Only requests that satisfy these checks are permitted. After these requirements for access are met, examine any data objects you permitted to pass as an added measure of protection.

The following examples illustrate how stringent policy enforcement can be more effective than relying on signature-based detection alone:

1. Few employees in any organization truly need the freedom to download or receive email attachments containing executable files, dynamic link libraries, zip/archive and Microsoft Cabinet (cabinet) files from any public Web site. And many spyware programs are downloaded as executable files. Implementing a security policy at a firewall that prohibits all employees except administrators from downloading or receiving "executables" effectively reduces the possibility that an employee will voluntarily or inadvertently install spyware, or be victimized by a mail-borne worm.
2. Adware and related tracking technologies are disruptive and invasive. Deploying a security policy that detects and strips cookies at a firewall provides more uniform and effective cookie transaction management than desktop browser and cookie defenses alone. A policy that blocks or denies domain name resolution for known adware sites (e.g., DoubleClick.com) may also defeat adware.
3. Even the most competent of search engine users can be misdirected or deceived into visiting a questionable Web site by a seemingly innocent query result. Employ a URL blacklist – or subscribe to a content service that maintains such lists for you – to block sites known to host spyware and prevent servers from falling victim to a "drive-by" spyware installation. One objective of attackers is to compromise accounts and systems and use these to spam or attack other systems. Policies that control the composition of email that originates from your trusted networks by limiting the number of email recipients; imposing a maximum mail message line, address length, and message size in any email; and authenticating mail users inhibits such mail abuses.

4. Certain remote administration, backdoor, and key logging 'trojan' programs use the DNS port for backchannel communication to a server. Employing a DNS proxy that detects protocol anomalies will block this illicit communication channel.
5. FTP is an easily abused protocol. Virus writers build FTP servers and clients into remote administration tools (RATs), trojans and backdoors to install additional attack tools on, and steal information from, compromised systems. Defining a security policy at a firewall that blocks downloads by content type, restricts commands available to users, whitelists approved FTP sites, and blocks unauthorized uploads by identifying directories containing sensitive information, may deter these attacks.
6. Unauthorized or improperly configured instant messaging and P2P applications can serve as conduits for malicious code, especially when these application permit file transfers to an organization's client computers from uncontrolled sources. These applications are sometimes difficult to block because they use HTTP. Defining a security policy that detects and blocks IMs and P2P applications or forces them to run on specific and auditable ports only during scheduled time periods controls traffic priority and limits bandwidth, and will contain this threat.

From these examples, it's easy to see how comprehensive user and application layer protection requires more than even the best signature-based solution alone offers. Why is this strategy not as highly publicized nor endorsed by vendors? Admittedly, it requires a more thoughtful policy definition and detailed implementation. But many commercial firewalls can't provide all the security features required to implement comprehensive, zero-day protection so they over-hype the features they do offer and gloss over those they do not.

WatchGuard Firewall® Pro and Intelligent Layered Security

The WatchGuard® [Fireware™ Pro advanced appliance software](#) and the Intelligent Layered Security (ILS) engine provide measures to counter malware of all forms, including viruses and spyware, without relying on signatures alone. Consistent with a defense-in-depth philosophy, WatchGuard® provides a comprehensive set of security services to offer zero-day protection, and complements these with [Gateway AntiVirus/Intrusion Prevention Service](#) (Gateway AV/IPS) that blocks suspicious network traffic and malicious code in real time.

Authentication and User-based Authorization

Comprehensive security begins with user authentication and user-based authorization. Fireware Pro supports RADIUS, LDAP, Active Directory and multi-factor SecurID® authentication using external servers. Administrators can allow or deny traffic (and objects carried within traffic) based on individual users or groups.

Applying the Power of Intelligent Layered Security

WatchGuard provides a comprehensive set of technologies within ILS to perform protocol anomaly detection, content type filtering, and control inbound and outgoing traffic and service use. Even a partial list of the extensive security features available through ILS illustrates how user-based authorization and policy enforcement through secure proxies effectively narrows a malware attacker's window of opportunity.

WatchGuard	Policies Properties
HTTP	HTTP requests Restrict URL length, request method, URL path, Web sites Enable authorization HTTP responses

	Restrict URL and total response length Deny or block according to content and body content types Strip cookies Block IM and peer-to-peer applications over HTTP Strip suspicious header fields
FTP	Impose length limits on usernames, passwords, filenames, etc. Restrict command operators (e.g., GET/PUT/PASV) Restrict downloadable content types Block uploading of sensitive material by file, type, and origin directory
SMTP	Impose length limits on recipient lists, email addresses Impose size limits on message bodies and attachments Rewrite Message ID and Server replies to hide private email server Restrict unsafe mail commands Restrict 8-Bit and binary MIME characters (buffer overflow protection) Require SMTP authentication Attachments Block, strip, lock, or scan attachments for malicious code Strip file attachments based on name and directory Mail addresses Block source routes and 8-bit characters in "From" fields Field substitution
DNS	Restrict DNS operators, query types Block or deny name resolution of prohibited sites

Table 1: User-based authorization and policy enforcement through secure proxies

Expand Your Arsenal with Gateway AV/Intrusion Prevention Service and Stateful Dynamic Packet Filtering

Proxies are one of many weapons in the ILS anti-malware arsenal. WatchGuard firewalls provide several complementary security options to help administrators build defenses against malicious code and network intrusions.

Gateway AntiVirus/Intrusion Prevention Service is an easy-to-manage, signature-based, integrated security option that identifies and blocks suspicious network activity and malicious code in real time. Gateway AV/IPS gives you an additional layer of protection against threats including viruses, spyware, keyloggers, backdoors, denial-of-service agents (zombies) and more.

Stateful dynamic packet filtering protects applications that are latency or jitter-sensitive. Organizations can control application quality of service (traffic priority, bandwidth and connection rate limiting) using dynamic packet filters. For other, non-proxied traffic, dynamic filters are applied according to service type and conditions surrounding the initiation of a connection. Organizations may define an approved time schedule for use of a given service offered from a particular destination. In such situations, dynamic filtering adds and removes policies depending on network activity. Or, if a particular host attempts to connect to a port or destination it has no business connecting to, dynamic filters can be configured to automatically add that particular host to a blocked sites list.

Early Detection and Blocking: More than Simply Signatures

All malware experts agree: blocking malicious code is far simpler and less costly than removing it. Experts also agree that the malicious code is a constantly-evolving threat that cannot be mitigated using signature-based detection alone.

A comprehensive defense against malicious code requires a thorough investigation into the root causes of infections and infestations. These results commonly reveal that overly permissive access poses a meaningful threat and opens too many vectors to attackers. Organizations must first define a security policy that offers the strongest possible defense against malware, and then choose a security gateway that provides all the measures and layers necessary to implement that policy.

Organizations that measure and address the malicious code threat in this manner will find that WatchGuard Fireware Pro and ILS measure up to the task. WatchGuard Fireware Pro and ILS is a powerful combination. By applying advanced proxy technology, user- and role-based policy definition, and state-of-the-art intrusion prevention, organizations of any size can deploy a defense in depth against malicious code threats that large enterprises using 'lesser' firewalls will envy.

For more information about WatchGuard security solutions, visit us at www.watchguard.com or contact your reseller.

Core Competence provides Internet, broadband, security, and wireless LAN consulting services from offices in Pennsylvania and South Carolina. Their staff is made up of respected and widely published experts in routed and switched internetworking; wireless LANs and WANs; 802.11 WLAN security; secure remote access and VPNs; firewalls, IDS, IPS; network and system security architecture and design. Core Competence received a fee for the preparation of this industry report.

ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:

www.watchguard.com

U.S. SALES:

+1.800.734.9905

INTERNATIONAL SALES:

+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of unified threat management (UTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. All products are backed by LiveSecurity® Service, a ground-breaking support and maintenance program. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please visit www.watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features or functionality will be provided on an if and when available basis.

©2006 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, Firebox, Fireware, Peak, Core, LiveSecurity, and Stronger Security, Simply Done are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part. No. WGCE66284_081007