

the Web Security report

A MESSAGING MEDIA PUBLICATION • SEPTEMBER 2006 EDITION • WWW.WEBSECURITYREPORT.COM

ABOUT THIS PUBLICATION

The Web Security Report acts as a publishing partner for Internet security solutions providers, testing labs, research entities and trade organizations. Published monthly by Messaging Media, LLC, the Web Security Report has an online and print audience of over 120,000 readers
publish@websecurityreport.com

906

Malware Trends: The Attack of Blended Spyware Crime

By **Pat Peterson**

Spam, viruses, phishing and spyware all have one thing in common. These are tools used by illicit business organizations to generate profits. Profits that are made at the expense of the global Internet community. The activities of these organizations range from unwanted marketing (in the form of spam and pop-up ads—questionable tactics to sell legitimate products), to outright fraud (by stealing credit card numbers, account numbers, passwords and other forms of sensitive corporate data).

FBI Investigates Costly Crime

Recently, the United States Federal Bureau of Investigation (FBI) issued a study concluding that the profits generated by these illicit organizations can be measured in billions of dollars annually, and that online crime has grown larger than the drug trafficking industry. While the numbers are hard to quantify, it is not hard to believe that these organizations are professionally run, highly organized and frequently operating at a global level. As a result, these organizations have the resources to develop very sophisticated tactics and technology that are collectively known as “malware”.

Malware costs enterprises around the globe billions of dollars every year. These costs come mainly in the form of disruptive side effects—IT help desk requests, desktop cleanup and remediation, system resource consumption. On top of these very real costs, there are significant intangible costs associated with private data being lost or compromised, as well as the negative PR associated with this type of security breach.

> *continued on page 2*

TABLE OF CONTENTS

Malware Trends: The Attack of Blended Spyware Crime	1
The Business Impact of Malware	6
Product Shootout Preview	10
Web Security News	12
Sponsor Profile	14
In This Edition	16

in the next issue

Bluecoat vs. IronPort Network Testing Labs and the Web Security Report will present the telling results of a head-to-head product comparison of gateway-based, anti-spyware solutions from Bluecoat and IronPort. In this issue, journalist and author Barry Nance provides a preview (see page 10).

Regular features include: Web Security News, Company Spotlight and Sponsor Profile.

SPONSORED BY
IRONPORT SYSTEMS



IronPort Systems, a leading Internet gateway security company, reports that more than 50 percent of corporate desktops are infected worldwide. The tactics employed by the authors of these threats have also become increasingly sophisticated, the latest being a “blended threat”—which combines spam, virus and spyware tactics into a single, well coordinated attack.

Malware Defined

Malware comes in a wide range of forms but they share one thing in common—they are pieces of unwanted code that embed themselves on an end-user PC without the end-user’s explicit knowledge. The types of malware discussed in this report include:

- adware
- tracking cookies
- browser hijackers
- Internet dialers
- keyloggers
- rootkits
- Trojan horses
- worms
- viruses

*“Storing data [like cookies] in a user’s computer can only be done if:
1) the user is provided information about how this data is used; and
2) the user is given the possibility of denying this storing operation.”*

Source: The 2002 European Union Telecommunication Privacy Directive

Given these numerous variants—and insidious infection methods, such as drive-by downloads and piggyback attacks—it is not surprising that malware has become such a widespread epidemic.

The most common form of malware is called **adware**. These are pieces of software that monitor the behavior of end-users and display Web-based advertisements that relate to the end-user’s activity. In most cases the products being advertised are legitimate—and are often large well known brands like Verizon, Citigroup or AT&T. However, these companies are rarely directly responsible for the adware deployment. The spyware comes from advertising networks or “affiliates”, which sell large blocks of end-user impressions to the ad agencies that represent these large consumer brands.

Another class of adware is a mechanism known as **tracking cookies**. A cookie is a data structure that stores information about a user on their PC. Websites routinely make use of cookies to keep track of the session state of a user’s Web browsing. The original design intent of a cookie was to enable the familiar “shopping cart”, which allows users to accumulate items to be purchased from multiple different webpages, possibly over the course of several visits. As is often the case with Internet technologies, the applications and use of cookies has extended well beyond the original intent. In 2000, the United States government enacted strict guidelines about the use of cookies—after it was disclosed that the Drug Enforcement Agency (DEA) used cookies to track computer users viewing its online anti-drug advertising (to see if they then visited sites about drug making and drug use). In 2002, privacy activist Daniel Brandt found that the Central Intelligence Agency (CIA) had been leaving persistent cookies on computers for ten years. When notified it was violating policy, the CIA stated that these cookies were not intentionally set and stopped setting them. On December 25, 2005, Brandt discovered that the National Security Agency (NSA) had been leaving two persistent cookies on visitors’ computers, due to a software upgrade. After being informed, the NSA immediately disabled the cookies.

The 2002 European Union Telecommunication Privacy Directive contains rules about the use of cookies. In particular, Article 5, Paragraph 3 of this directive mandates that storing data (like cookies) in a user’s computer can only be done if: 1) the user is provided information about how this data is used; and 2) the user is given the possibility of denying this storing operation. However, this article also states that storing data that is necessary for technical reasons is exempted from this rule. This directive was expected to have been applied since October 2003, but a December 2004 report indicated that this provision was not applied in practice, and that some member countries (Slovakia, Latvia, Greece, Belgium, and Luxembourg) did not even transpose it. The same report suggests that a thorough analysis of the situation in each of the member states should also be conducted.

While cookies are a necessary component of many websites, tracking cookies are designed to track a user's behavior across multiple sites. Spyware sites and illicit marketers will routinely use tracking cookies to monitor specific behavior of an end-user and associate it with personal information like name, credit card number and other private information. This information can then be harvested and sold to other illicit marketers to create more spam, pop-ups and other disruptive forms of marketing.

Another form of spyware is the **browser hijacker**. A browser hijacker will change the settings on an end-user's browser and redirect the browser home page, mis-typed URLs and other requests to undesirable sites. One of the first browser hijackers was Cool Web Search (CWS) which redirected invalid URLs to its own search engine, and presented the user with its own sponsored links. CWS was very difficult to remove and extremely widespread. Thus, many new browser hijackers are often referred to as CWS. Some modern browser hijackers will redirect a site to a page that reads, "Warning: your PC is infected with spyware"; and won't release that page until the user purchases a "spyware removal" package of questionable value. Browser hijackers can permanently impair a browser, inhibiting a safe Internet experience.

An **Internet dialer** is another tool used by illicit marketers. This is a piece of code that will access a PC modem in the background and quietly make calls to pornographic websites or 1-900 numbers, which can result in huge telephony charges for the end-user. These threats apply to users with a modem connected to an active phone line.

A **keylogger** or system monitor is a much more dangerous form of spyware. These programs will silently install themselves and monitor the key strokes and system events of an infected PC. Keyloggers can be combined with sophisticated logic to perform tasks such as looking for the address of an online bank, recording the username and password, and then transmitting this information back to a rogue server—which in turn can transfer funds from the affected user. Keyloggers can also be used to harvest sensitive corporate information. A keylogger placed on the machine of a CFO or CEO could readily access

corporate earnings data prior to earnings announcements, creating a trading opportunity worth billions of dollars. A keylogger has access to every application—it can obtain information from webpages, emails and database interactions.

The FBI used a keylogger to obtain the PGP passphrase of Nicodemo Scarfo, Jr. He pleaded guilty to running an illegal gambling operation in 2002 ("Mobster's son pleads guilty of gambling; computer spying helped seal case" Associated Press, 1 Mar 2002). The FBI has also reportedly developed a Trojan horse-delivered keylogger program known as "Magic Lantern". These keyloggers were used for law enforcement, but they illustrate the very real power and potential destructive force of rogue keyloggers and system monitors.

Another extremely dangerous form of malware is a "**rootkit**". A rootkit is a piece of software that attaches itself to the core operating system in order to bypass system security restrictions. Every operating system relies on application program interfaces (APIs) to function. A call to open a file is an API call. A rootkit allows these APIs to be manipulated. Thus when the operating system requests a particular file, the rootkit could return any other data object. This level of control is almost impossible to counteract. Rootkits can disable any desktop-based security software. They are extremely difficult to detect, and often designed to preserve and reinstall themselves.

In 2005, Sony BMG music distributed CDs that surreptitiously placed a rootkit on Microsoft Windows PCs when the CD was played on the computer. Sony provided no mention of this in the CD or its packaging, referring only to security rights management measures. This controversy touched off a public outcry that resulted in a large-scale consumer settlement.

————— > [continued on page 4](#)

A Trojan horse is a form of malware that infects a machine by posing as another harmless piece of software. As an example, a Trojan could be delivered by a website that offers enticing content (such as a music video) which requires a special video codec plug-in to Windows Media Player. When the user downloads the codec plug-in they also get a Trojan which silently installs itself on the targeted PC. To avoid detection, a Trojan will often not contain any harmful code. Instead, it will install itself and then load malicious code from a remote Web server, sometimes using network ports other than Port 80 (the standard HTTP port). Trojans are different from viruses or worms in that they do not propagate on their own, they require “social engineering” to trick the user into running them. However, the rapidly expanding universe of Web content and applications continues to create new opportunities for clever Trojan horse programs.

A worm is a form of malware that propagates itself. Several worms (such as “Slammer”) have made front page news in recent years by flooding networks with traffic and causing widespread outages. A worm usually takes advantage of a security flaw to install itself on a host PC. Once installed, it then scans the network—looking for other machines that have the same security flaw. Using this method, a single worm can create large-scale propagation in a matter of hours.

The word “**virus**” tends to be a catch-all for any form of malware. But, in technical terms, a virus is a hostile piece of code that replicates by inserting copies of itself into other code or documents. According to ICSA Labs (a security industry consortium, formerly known as the International Computer Security Association), more than 90 percent of all viruses spread via email. Email-borne viruses have an attachment that may pose as a legitimate file, but actually contains a harmful executable. One of the more clever viruses propagated in the form of a password protected .zip file, making it very difficult for traditional anti-virus software to detect. The email was designed in a manner that enticed the end-user to enter a password and thereby infect their machine. Once infected, a machine can be used

for any number of purposes, including acting as an SMTP email server (which can be used to send out more copies of the virus—and then later to send out spam). These infected computers are often organized into groups, called “botnets”, and are a key tool in the delivery of malware.

Getting Infected

Malware needs to be loaded onto a targeted PC. There are several ways this can happen.

One insidious form of infection is called the “**drive-by**” download. This term is used to describe the loading of an executable onto an end-user PC, without the user’s knowledge. In the strict definition of the term, the malware would be using a security flaw in a browser program to achieve the download. However, the common use of the term includes the unwitting download of code because an end-user was tricked into clicking on an ad or pop-up.

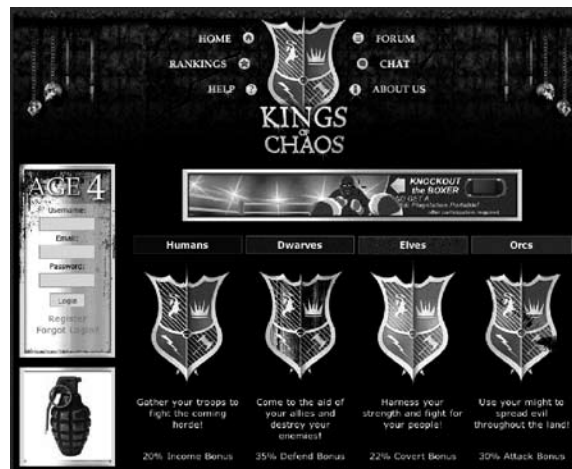


Figure 1: Kings of Chaos, a legitimate gaming site that delivered spyware.

An example of a drive-by download once victimized kingsofchaos.com and its visitors. This is a legitimate site that makes money by serving ads. The ad content comes from a different server—in this case adworldnetwork.com, a legitimate ad network. A drive-by download was made possible because the ad itself contained an inline JavaScript program, which loads HTML from the ad provider. This code also loaded a browser hijacker and pop-up ad server via an exploit in Internet Explorer.

More common than the drive-by download, a “piggyback” attack occurs when malware is embedded in an executable that would otherwise be harmless.

A 2006 study, performed by Dr. Steven Gribble at the University of Washington, crawled the Web looking for infected content in a piggyback attack. The study crawled more than 20 million webpages and found over 20,000 unique executables. An astounding 1 in 20 of these executables contained piggybacked malware of some type. Furthermore, the malware was not limited to rogue sites. 1 in 25 sites was infected, often through “affiliations” like the one described earlier with kingsofchaos.com. The thousands of infected executables discovered contained only 89 different forms of malware. However, each infected executable would require a separate anti-malware signature (because each had the malware “packed” in a unique executable). The malware was using the host executable as camouflage to avoid detection by a traditional signature-based system. Malware distributors tend to avoid high profile, trusted sites. The categories of sites found with piggybacked malware are listed in Figure 2.

The infections were found to be clustered on a small number of heavily infected malware sites, but the distribution had a long “tail”—which means there are a large number of sites that have only a few pieces of malware on them. This suggests that the first generation approach of creating a “URL blacklist” is

ineffective because there is a very large population of legitimate sites that have some type of malware.

The occurrence of the more dangerous drive-by download was much lower than the piggybacked download, with 0.04 percent of the 20 million pages launching an attack. However, given the very malicious nature of a drive-by download, the payload tended to be more dangerous. Thus, drive-by downloads are still a major problem on the Internet.

Sites that launched a more malicious drive-by download had a different profile than the piggybacked sites. These sites are less likely to be legitimate, and more likely to be engineered for malicious intent. The distribution of these sites by category is shown in Figure 3.

Pat Peterson is the Vice President of Technology for IronPort Systems. He has written numerous articles for a variety of publications and is a frequent speaker at industry events.

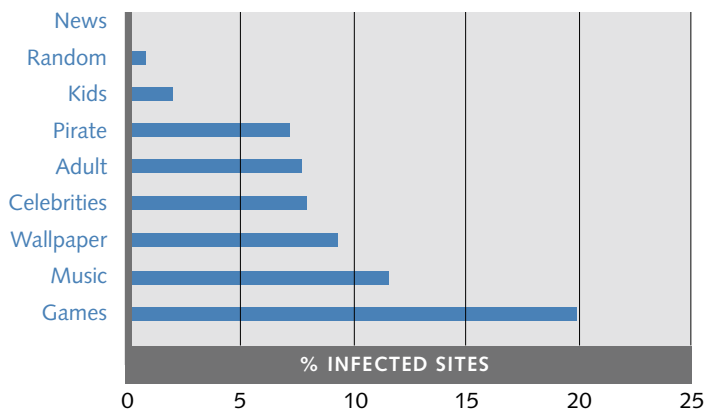


Figure 2: Piggyback Infected Sites by Category

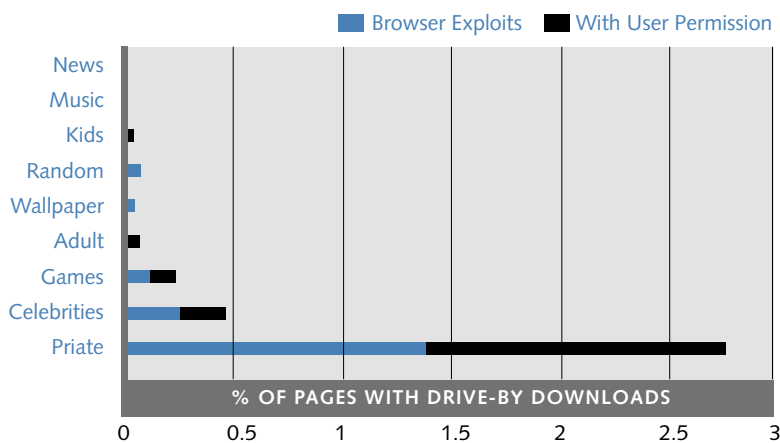


Figure 3: Drive-by Sites by Category

This figure illustrates that more than half of the drive-by downloads occurred without initiating any type of notification to the end-user. Thus, a user with the misfortune of typing an incorrect URL (a classic was www.google.com) may well hit a site that could infect their machine without any indication.

The Business Impact of Malware

By The IronPort Threat Operations Center and WSR Staff

IronPort Systems recently released a study of malware infection rates in the enterprise. This study found that more than 50 percent of corporate PCs were infected with some type of malware. Of these infected machines, adware and tracking cookies were clearly the most prevalent infections, but Trojans and system monitors represented over 7 percent of the infections—a shockingly high infection rate given the malicious nature of these two types of threats. A detailed breakdown is shown in Figure 4.

	ADWARE	TROJANS	SYSTEM MONITORS	TRACKING COOKIES
Global Infection Rates	48%	7%	5%	77%
North America	66.72%	9.75%	6.96%	89.39%
UK	46.35%	6.77%	4.84%	74.48%
Germany	43.27%	6.32%	4.52%	69.53%
France	38.69%	5.65%	4.04%	62.17%
Japan	43.37%	6.34%	4.53%	69.69%
China	55.32%	8.08%	5.77%	88.9%
Australia/New Zealand	39.88%	5.83%	4.16%	64.09%
Other	49.73%	7.26%	5.19%	79.91%

Figure 4: Enterprise Infections by Type of Malware and Geography

Infection rates were fairly similar across geographies, and by company size. Malware is a problem that effects all Internet users.

This is despite the fact that more than 65 percent of these same enterprises surveyed had deployed some type of desktop-based anti-spyware or anti-virus system. Clearly, these first generation malware defenses are not sufficient to protect corporate networks.

The enormous business impact of this level of malware is not hard to imagine. Any consumer with a PC has probably had a similar experience—the PC strangely seems to slow down, though the hard drive is thrashing or a browser won't start reliably, and the entire system becomes unstable. Sweeping with multiple client-based solutions doesn't seem to fix it. Once malware gets installed, it is very difficult to remove. In the case of rootkits, the only practical remedy is to reinstall the operating system.

Consider an extremely conservative view of the business impact. Assume that only the most malicious forms of malware—keyloggers and system monitors—require complete attention. These malicious forms of malware make use of rootkits and other obfuscation techniques as described earlier, and thus require a reload of the operating system to remedy. For a 2,000 seat enterprise, 3.5 percent or 70 systems would require an O/S reinstall. This takes an average of four hours (at a rate of \$75/hr for IT staff), plus four hours of lost employee productivity. Assuming the employees are equally valuable as their IT counterparts, this translates into \$600 per infection—\$42,000 just to repair those 70 systems. Next, assume that systems infected with adware and tracking cookies can be repaired with client-based tools and minimal IT staff support. This takes an average of one hour of IT time plus one hour of lost productivity, which translates into an additional \$135,000. That

brings the total (for cleaning the entire population) to \$177,000. Considering that new strains of malware are introduced daily, it is not hard to see how this cost becomes a recurring drag on corporate IT resources. In its study of enterprise IT teams, IronPort found that malware costs over \$150 per PC user per year. This number only reflects the direct IT costs associated with control and removal of malware, it does nothing to consider the billions of dollars at stake if confidential information is leaked or lost due to malware infections. Since the cost of deploying and managing advanced malware defenses is significantly lower than the cost of repairing damage done by malware infection, the old adage holds true—an ounce of prevention is worth a pound of cure.

Preventing Malware Infections

Malware defense systems bear a strong resemblance to the anti-virus solutions that have been widely deployed and are now considered mature. This includes multi-layer, best-of-breed defenses—with protection at the desktop, in the network core and at the perimeter. Desktop solutions for anti-malware have been in existence for some time, with every major anti-virus vendor offering anti-malware protection to address modern threats like keyloggers and Trojans. There are also specialized providers, which offer best-of-breed desktop solutions focused specifically on spyware. These providers have been able to post impressive results—sometimes offering twice the catch rates—of the incumbent anti-virus solutions that have been updated to address spyware.

The Buying Criteria for Anti-Malware Solutions

Perimeter-based anti-malware solutions are much less mature. Consequently, they are worthy of discussion. There are four basic processing approaches for perimeter-based malware defense—network-based, proxy-based, list-based and signature-based systems. All four approaches have their own strengths and limitations. The best solutions in the industry take advantage of all four types of processing.

Network-Based Systems

Network-based systems operate at the packet level. They can either be inline or non-inline (on a span tap or other network connection point). Because they are not fully rendering the content, but rather inspecting the pieces of data as they go past, these systems are typically very high performance. They also have the advantage of being able to analyze all network traffic types, not just the traffic of a specific protocol.

Network-based systems are excellent at detecting malware attempting to “phone home”. When a Trojan downloader is installed, it will attempt to connect to an illicit server in the network and download the more malicious code such as keyloggers, SMTP spam engines, or other malware. Often these Trojans will attempt to find open ports in the network that do not have the defenses in place that Port 80 (the HTTP port) or Port 25 (the SMTP port) typically do.

The primary disadvantage of network-based systems is their inability to view traffic at the application layer. Consequently, a malicious piece of code that is piggybacked on another piece of code will typically avoid detection because (when examined, packet by packet) the malicious code is camouflaged.

Proxy-Based Systems

A proxy is an application server that sits between the end-user and the server they are trying to reach. A Web proxy receives an outgoing request from a client and then initiates a new connection with the target site on behalf of the user. Server responses are directed to the proxy, which in turn shuttles each response through to the end-user. The proxy is an ideal filtering agent because it fully understands the HTTP protocol and can perform a complete examination of the content.

—————> [continued on page 8](#)

In its study of enterprise IT teams, IronPort found that malware costs over \$150 per PC user per year.

List-Based Systems

Many of the current vendors of anti-malware solutions have their roots in acceptable use policy (AUP) enforcement. These systems created lists of URLs that were classified by content type—adult, games, sports, etc. This allowed corporate IT managers to enforce acceptable use policies by blocking undesirable site access. These systems generally used some type of manual site classification which created a large database of classified URLs. Since legitimate websites don't change all that often, these databases were updated periodically, maybe daily or weekly. List-based AUP filters can be deployed on either network-based or proxy-based systems.

List-based systems are an effective part of an overall malware defense. They also have the advantage of combining their legacy acceptable use filtering with newer anti-malware filtering. However, they are also subject to some very significant shortcomings.

List-based systems, by definition, are reactive. A piece of malware is served from a particular system—and detected by some type of detection mechanism. The database will then be updated and pushed out to remote systems in the field. This process can

range from a minimum of several hours to a more typical response, measured in days. With malware authors creating dynamic attacks that persist on a bot machine for only a

matter of hours, most list-based systems are too slow to react. Another drawback of list-based systems is that they only “map” or have values for a very small percentage of the Internet—usually about 10-20 percent. Thus, for the vast majority of Web servers on the Internet (as well as short-lived websites and bots—the most typical malware infection vectors), a list-based system has no information.

A Web reputation system measures the traffic patterns and characteristics of virtually every active Web server on the Internet.

An interesting offshoot of a list-based system is the emergence of Web reputation systems. A Web reputation system measures the traffic patterns and characteristics of virtually every active Web server on the Internet. As opposed to a list-based system that maintains a simple allow or block verdict, a reputation system assigns a score of -10 to +10 to each URL measured. State of the art Web security appliances can then use this score to dynamically determine how to handle incoming traffic. Bad traffic is blocked, questionable traffic is scanned by a signature-based system, and good traffic bypasses signature scanning to conserve system resources and minimize end-user latency.

Reputation-based systems overcome the reaction time problem by having a score for virtually every active URL on the Internet. So, if a new Web server just appeared and is receiving relatively high volumes of traffic, a reputation system will assign a neutral or slightly negative score—which will force the incoming content to be signature scanned. If the new Web server is exhibiting extremely suspicious behavior, such as sudden volume spikes emanating from an IP range known to be made up of consumer broadband networks (which don't typically host legitimate Web servers), the initial reputation will be negative and the content will be blocked. This type of intelligent initial assessment effectively overcomes the reaction time issue of list-based systems. Because of their ability to effectively clamp down on dynamic network hopping threats, reputation-based systems revolutionized the network security market—with virtually every leading vendor now claiming some type of reputation system.

One key attribute that drives the effectiveness of a reputation system is the size of the underlying database. In order to accurately measure the volume and behavior of virtually every active Web server on the Internet, a security vendor needs to sample Internet traffic on a very large scale—such as 10 or 20 percent—around the globe. There are very few vendors that actually have access to this type of traffic, and they tend to be vendors that have a mixture of ISP and enterprise customers. Although

every security vendor on the market will claim to have a reputation system, the actual efficacy of these solutions will vary widely in accordance with the size of the underlying database.

Signature-Based Systems

Signature-based systems are the mainstay of traditional anti-virus programs. These systems create a digital “fingerprint” of the bit patterns associated with known malicious code. They are very accurate, yielding near perfect results (catch rates in excess of 99 percent with false positive rates of one in one million or less). Yet, if these systems are so powerful, why do computer viruses and malware remain a problem? Signature-based systems have two major drawbacks. The first of these is reaction time. When a new exploit occurs, a signature vendor needs to detect and isolate the threat, develop the signature, and push it out to the millions of systems that use it. This process takes anywhere from hours to weeks, depending on the complexity of the outbreak. Furthermore, the response times of all major vendors vary widely. This is why most enterprise security teams have deployed a multi-vendor, multi-layer defense—if one signature vendor is slow to react, hopefully another will be faster. An excellent resource for measuring the response times of leading anti-virus vendors is a website maintained by IronPort Systems, www.ironport.com/toc.

The other major challenge with signature-based systems is performance. As malware has grown increasingly sophisticated, the size of leading signature engines has grown exponentially. Throughput of industry leading spam filters has dropped more than 60 percent in the past 12 months. The vast majority of anti-malware signature scanning takes place at the email gateway or at the desktop, neither of which are highly sensitive to performance. But the Web is a real-time protocol. Consequently, introducing signature-based scanning at the Web gateway creates serious performance issues. Traditional signature-based systems will add several seconds of latency to each page load. For the end-user, waiting for that page to load, the impact is significant—it

can feel like a modem instead of a high-speed data link. This sensitivity to latency creates an important subtlety. Latency (the time required to scan a single object) and throughput (the total number of objects that can be scanned) are related. As the system gets busy, latency increases. But the performance penalty associated with signature scanning often introduces unacceptable latency, even when the system is not busy, because performing a single scan takes time. For this reason, enterprises both large and small have avoided widespread deployment of signature-based scanning systems on HTTP traffic.

Although every security vendor on the market will claim to have a reputation system, the actual efficacy of these solutions will vary widely in accordance with the size of the underlying database.

Summary

Malware is the newest, and therefore one of the most sophisticated, threats to Internet communications. Anti-malware systems are still in their infancy and have lots of room for innovation and improvement. Deploying these types of systems at the Web gateway poses a series of technical challenges that no previous solutions have had to overcome. Furthermore, a state of the art system will need to incorporate the best attributes of the four different classes of solutions currently available. While all the technical challenges are surmountable, relatively few vendors have the vision or resources to pull all the pieces together. Fortunately, it is reasonable to predict that a few will—as the business imperative to deploy a highly accurate, enterprise class perimeter-based anti-spyware system is at an all time high. ■

We look at **TWO NEW** gateway-based anti-spyware solutions from IronPort and Bluecoat.

By **Barry Nance**, Network Testing Labs

Malware can cost your company the time, effort and expense of extricating its residue from infected computers. A study by The Radicati Group, entitled "Corporate Anti-Spyware Market, 2005-2009," indicates that the number of anti-spyware tool licenses will increase from 16 million in 2005, to over 540 million in 2009. Companies are concerned about spyware's security risks, regulatory compliance and employee productivity losses. The study also reveals that the administrative cost of dealing with spyware-infected computers will quickly rise as spyware programs become increasingly devious, reaching about \$265 per user in 2005.

To find out which anti-spyware product is best, we tested IronPort Systems' S-Series appliance and Bluecoat's SG-8000 appliance. The most important criteria in our evaluation was the ability to identify and thwart all (or virtually all) spyware. We also looked for useful reports, timely alerts, ease of use and ease of deployment. Protecting our network from users who roam the Internet too freely was our goal.

Smart Gateways

Stopping spyware via gateways at each Internet connection point is clearly superior to cleaning it off individual servers and desktop computers. A gateway is simpler to administer, users can't fool with it, and desktop machines and servers don't have to shoulder the extra burden of detecting and removing spyware. To the extent that a gateway filters every single crumb of spyware, and users do not bring freeware or shareware software into the office, the gateway approach is an ideal anti-spyware solution.

In our review, we discovered which product is the best anti-spyware gateway. We scored the anti-spyware solutions using six categories, giving each category the weight shown in parentheses:

- Malware identification/blocking (40%)
- Additional features—stopping "phone home," definition update frequency (15%)
- Performance (15%)
- Reports and SNMP alerts (10%)
- Ease of use and deployment (10%)
- Documentation (10%)

The table below identifies five common types of spyware.

CATEGORY	TYPICAL ACTION
Keylogger (AKA Trackware)	Captures keystrokes (including personal information and passwords) and/or tracks the websites you visit.
Trojan	Delivers malicious software bundled with useful or seemingly benign software.
Droneware	Sends spam and/or turns your PC into a host for offensive Web images.
Dialer	Auto-dials area code 900 and/or other expensive, long distance calls via your modem.
Adware	Pops up unsolicited and annoying advertisement-laden browser windows and/or hijacks your Internet search (Yahoo, Google, etc.) results.

How We Did It

Focusing on these two new gateway products, we primarily looked for the ability to identify and block malware (such as keyloggers, browser hijackers, adware, rootkits, dialers, data miners and Trojans). We wanted a product to prevent malware from sending data from our network (i.e., “phoning home”), identify already-infected clients, handle Skype- and IM-borne malware as well as HTTP-borne malware, scan traffic quickly, receive frequent spyware definition updates, integrate with a network management system (such as OpenView) and produce helpful reports on infection attempts and traffic statistics.

We collected a suite of 70 malware samples and vendors gave us some additional samples to test with. We moved the collected material to an isolated, quarantined network.

The quarantined network consisted of three subnets.

SUBNET 1 had 10 client machines with a variety of operating systems, including Windows NT, 98, 2000, ME, XP, Red Hat Linux and Macintosh OS X.

SUBNET 2 contained three Web servers (Microsoft IIS, Netscape Enterprise Server and Apache), three email servers (Exchange, Notes and Sendmail), two file servers (Windows 2003 Advanced Server and Netware) and two database servers (Oracle 8i and Microsoft SQL Server).

SUBNET 3, simulating the “Internet,” had Web, IM and Skype servers and clients containing the malware instances and sporting “bad guy” IP addresses and URLs. Systems on the first two subnets accessed the third subnet as if it were the actual Internet.

To measure performance, we used two time-synchronized protocol analyzers on the Internet and local network sides of the gateway device and examined the resulting packet captures to know the time taken by a device to forward or discard each network message.

Each gateway product connected our two client subnets to our simulated “Internet”. Client and server machines started off in a pristine state for each test.

Our clients and servers attempted to download malware from the simulated “Internet.” We noted how well the products identified malware traffic and blocked attempts by the malware to send data back to the source. We gauged success or failure by examining each machine for malware after each test. We looked for running malware processes, new program files (EXE, DLL or OCX, possibly marked with the hidden attribute) and directories as well as Registry and Start Menu changes.

We think you’ll be vitally interested in the results of our review to be published online (at www.websecurityreport.com) in early October. For more information, please contact: editorial@websecurityreport.com. ■

About the Author

Barry Nance is a networking expert, magazine columnist, book author and application architect. He has more than 29 years experience with IT technologies, methodologies and products. You can email him at barryn@erols.com.



About Network Testing Labs

Network Testing Labs performs independent technology research and product evaluations. Its network laboratory connects myriads of types of computers and virtually every kind of network device in an ever-changing variety of ways. Its authors are networking experts who write clearly and plainly about complex technologies and products.

McAfee, Inc. Reports: Celebrity Websites Most Prolific Distributors of Adware

McAfee research shows that adware and spyware distributors abuse the affiliate marketing programs of legitimate companies. In addition, adware distributors use front companies and websites to reach unsuspecting users and intermediaries—meaning that legitimate sites are finding themselves tied to known spyware distributors. Programs then

install themselves on a user's machine, often as the trade-off for a piece of "free" software, and are used to collect marketing data and distribute targeted advertising.

To learn more about adware, spyware and the top potentially unwanted programs rated by McAfee, visit: www.mcafee.com/us.

Webroot Reports: Spyware Infection Rates Return to Peak 2004 Levels

During the second quarter of 2006, Webroot researchers found that 89 percent of consumer PCs were infected with an average of 30 pieces of spyware—a slight increase from the first quarter of 2006 when infection rates returned to alarmingly high levels (after a supposed lull in spyware infections during the second half of 2005). According to the report, new distribution channels, advanced spyware technologies and a reliance on free anti-spyware programs are all contributing factors to the startling increase.

"Less than a year ago, many so-called Internet security experts began claiming that spyware was on the decline and that infection rates would soon drop to the point of extinction," said C. David Moll, CEO of Webroot Software. "Spyware is a financially motivated threat and as long as there is a dollar to be had, cyber criminals will do everything possible to steal it."



The complete State of Spyware Report is available at: www.webroot.com/sosreporhome.

FTC Closes Door on Spyware Operation

An operation that placed spyware on consumers' computers, in violation of federal laws, will give up more than \$2 million to settle Federal Trade Commission charges.

The order names Enternet Media Inc., Conspy & Co. Inc., Lida Rohbani, Nima Hakimi, and Baback (Babak) Hakimi, all based in California—whose software codes were "Search Miracle," "Miracle Search," "EM Toolbar," "EliteBar," and "Elite Toolbar."

Under a stipulated final judgment and order, the defendants are permanently prohibited from interfer-

ing with a consumer's computer use. The defendants also are permanently prohibited from making misleading representations regarding the nature or effect of any type of software code, file, or content.

The FTC's case was brought with the assistance of the Microsoft Corporation, Webroot Software, Inc. and Google Incorporated.

More information about this order can be found at: <http://www.ftc.gov/opa/2006/09/enternet.htm>.

GRISOFT Launches Beta Program For New Comprehensive Anti-Malware Security Suite

GRISOFT extends its security offerings for small business users into beta programs by adding AVG Anti-Spyware and AVG Anti-Malware, which integrates anti-virus and anti-spyware features.

Beta versions of AVG 7.5 products are designated for compatibility testing in large number of different hardware and software configurations in Windows

XP, Windows Vista Beta 2/RC1, FreeBSD and GNU/Linux operating systems.

Beta versions of AVG products are available for testing, free of charge, at: beta.grisoft.cz.

Ask the Experts: Larry Clinton - Internet Security Alliance

On the eve of his testimony before a congressional subcommittee, Larry Clinton, COO of the Internet Security Alliance spoke to editors at Web Security Report about the need for economic incentives as a "powerful mechanism encouraging corporations to use best practices" pertaining to cyber security. He also commented that any improvement to cyber security fundamentally "benefits national security" and the fight against terrorism.

A webcast of the September 13, 2006 hearing: "Cyber Security: Protecting America's Critical Infrastructure, Economy and Consumers," is available at: <http://energycommerce.house.gov/>.

To learn more about the mission and activities of the Internet Security Alliance, visit: www.isalliance.org.

company spotlight

Breach Security

Breach Security's products address both enterprise and governmental needs, using a unique combination of detection and prevention technology to secure business-critical Web applications from targeted cyber attacks. Breach, founded in 2004, is backed by southern California's leading venture capital firm, Enterprise Partners, and other A-list ventures. With headquarters in Carlsbad, California, sales offices across the United States,

and R&D facilities in Herzliya, Israel, Breach Security brings a global focus to today's Web security challenges. www.breach.com



IRONPORT SYSTEMS, the leader in Internet Gateway Security, has recently introduced the IronPort S-Series Web Security Appliance. This enterprise class solution delivers the industry's most comprehensive malware protection by integrating processing at both the network layer and at the application proxy layer. Furthermore, the IronPort S-Series includes a heavily optimized, high-performance signature-based scanning engine as well as the first Web reputation system.

Network-Layer Protection

The IronPort S-Series™ has an integrated Layer (L4) traffic monitor. This wire-speed device can sit inline or on a network tap. It monitors all network activity looking for malicious traffic that is trying to “phone home” or connect to a rogue server. The L4 traffic monitor shares data with IronPort's Web reputation system, to identify and stop malware before it does harm. The L4 traffic monitor also does an excellent job of identifying the most infected PCs on the corporate network—allowing IT administrators to proactively and efficiently launch desktop clean up efforts.

Proxy-Layer Processing

The IronPort S-Series also includes an extremely high performance Web proxy. Built on IronPort's proprietary operating system, AsyncOS™, the IronPort S-Series' proxy can support up to 100,000 simultaneous connections—as much as 10x more than traditional UNIX-based proxy servers.

Accelerated Signature Scanning

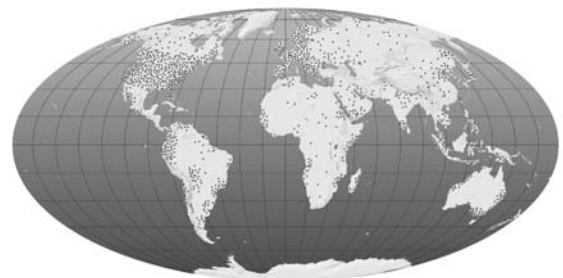
IronPort® developed its proprietary Dynamic Vectoring and Streaming™ (DVS) engine to accelerate the signature scanning of Web content and minimize latency. The DVS engine performs intelligent scanning and reputation-based caching to minimize the amount of scanning that actually needs to take place. When an object does need to be scanned, the DVS engine has a unique streaming capability. It can scan an object while simultaneously receiving the remainder of it and buffering it though to the end-user. The combination of intelligent scanning and streaming of data yields a decrease in latency that approaches 1/10th that of traditional signature-based systems. This makes the IronPort S-Series imperceptible to end-users.

The World's First Web Reputation System

IronPort invented the concept of reputation filtering more than three years ago. This capability is at the heart of the IronPort S-Series. For each Web request, IronPort makes an assessment of the reputation (or trustworthiness) of the URL requested. This reputation score is based on over 45 different parameters, including such factors as:

- How long has the domain been registered?
- What is the country of origin?
- What is the IP range of the hosting server?
- How does the name server infrastructure behave?
- How much traffic is the URL getting?

By analyzing these objective parameters the Web reputation system can make a very accurate determination about every active Web server on the Internet. Based on configurable thresholds, the IronPort S-Series will reject traffic that is clearly hostile—without wasting system resources on a full signature scan. Similarly, known good traffic with a sufficiently positive reputation score will bypass the DVS



Over 100,000 organizations participate in IronPort's SenderBase Network, enabling the world's largest email and Web traffic monitoring system.



The IronPort S-Series Web security appliance: Powerful malware protection enables the industry's most comprehensive perimeter defense.

scanning engine and move right through to the end-user. Traffic with a neutral or slightly negative score will be passed to the DVS engine for further analysis.

By creating a score for each individual URL, IronPort's Web reputation system can rectify an increasing problem. Legitimate websites (the most recent being myspace.com) will often host an ad through an advertising network. However, they do not control the content of the ad. Nefarious advertisers can come from a server that is two or three parties removed—an affiliate of an affiliate of the ad network. Sometimes these advertisers will use this mechanism to deliver malware to unsuspecting machines, even though the ad appeared on a legitimate, trusted site. Because IronPort's Web reputation system assigns individual URL scoring, the questionable ad would be given a neutral score and be sent to the DVS scanning engine—but the remaining objects on the page would be given a high score and be exempt from signature scanning.

This is an excellent example of how IronPort's Web reputation system maximizes system throughput, reduces latency and increases overall accuracy by as much as 20 percent.

Powered by IronPort's SenderBase

IronPort's SenderBase® is the world's first, biggest and best traffic monitoring network. SenderBase measures more than 25 percent of the world's messaging traffic, receiving over five billion queries per day. IronPort appliances are deployed at eight of the ten largest ISPs in the world, as well as more than 40 percent of the Global 100—the 100 largest corporations in the world. Having access to this type of traffic is a key differentiator for both SenderBase and IronPort. SenderBase is unique in that it even collects data from the

networks of organizations that are not IronPort customers. IronPort shares data with other large ISPs in a data peering relationship. Currently, there are over 100,000 different networks contributing data to SenderBase. This translates into the industry's most accurate reputation system. IronPort's Web reputation system can increase malware catch rates by more than 20 percent over signature-based scanning alone—an unprecedented increase in efficacy.

Enterprise Management Tools

Global corporations need powerful management and reporting systems to optimize their investment and minimize the required administration time. The IronPort S-Series is built on IronPort's proprietary AsyncOS operating system and thus it inherits the world class management and reporting capability that has made the IronPort C-Series™ the number one choice among enterprises for email security.

The IronPort Advantage

IronPort Systems is focused on building comprehensive gateway security for enterprise customers. IronPort is a clear leader in the industry, pioneering technical breakthroughs like reputation systems and very high performance proxy appliance designs. IronPort's industry-leading systems have a demonstrated record of unparalleled performance, accuracy and reliability. To secure greater protection for your company's messaging system, visit www.ironport.com or call 650-989-6530.



www.ironport.com

PAGE 1 Malware Trends: The Attack of Blended Spyware Crime

Sorting through the myriad of malware varieties and infection methods provides a view into how these Web-based threats have evolved to become so sophisticated and harmful.

PAGE 6 The Business Impact of Malware

Companies are quickly realizing that first generation malware defenses are not sufficient to protect their networks and now may be the perfect time to increase their protection investment.

PAGE 10 Product Shootout Preview

Learn about the criteria that Network Testing Labs will use to review gateway-based anti-spyware solutions from IronPort and Bluecoat. Then, stay tuned for the complete results—coming in the October issue.

PAGE 12 Web Security News

Your source for short takes on Web security tales, tools, tips and trends.

PAGE 14 Sponsor Profile

Web Security Report sponsor, IronPort Systems, is developing revolutionary technologies to help make the Internet safe.

THE WEB SECURITY REPORT

A Messaging Media Publication

BUSINESS OFFICES

Messaging Media, LLC
P.O. Box 643084
Los Angeles, CA 90064
Phone: 866-808-4200
Fax: 310-836-4067

ADVERTISING/SPONSORSHIP INFORMATION

Managing Partner: Tim Matteson
publish@websecurityreport.com
866-808-4200 (ext. 361)

the Web Security report

Messaging Media, LLC
10536 Putney Road
Los Angeles, CA 90064