

the Web Security report

A MESSAGING MEDIA PUBLICATION • APRIL 2007 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

407

Can We Make the Internet Accountable? Only If We Up The "Anti-"

TABLE OF CONTENTS

Can We Make the Internet Accountable? Only If We Up The "Anti-"	1
Web Security News	8
Sponsor Profile	10
In This Edition	12

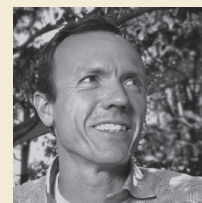
By Paul Gargaro

The threat from spam, spyware and associated malware is worse than ever.

Not long ago, it appeared the tide was turning in the battle against these Internet-based threats. State and federal legislators were paying attention, while network operators were actively engaged in ways to staunch their flow and eliminate the potential risks. On the spam front, in particular, the optimism was so great that by 2004, Microsoft's Bill Gates went so far as to proclaim that "the spam problem would be eliminated."

Accountability Advocate

Tom Gillis is the Chief Marketing Officer at IronPort Systems. In addition to frequent appearances on panels and television and radio news shows covering technology, Tom is also the author of the new book, *Upping the Anti- In Pursuit of the Accountable Internet*. Gillis' first book, *Get the Message – A Business Guide to Surviving the Email Security Crisis*, was highly regarded as a critical look at the state of email and its future. Tom has twenty years experience in the technology industry. Tom has an MBA from Harvard University, an MSEE from Northwestern University and a BSEE from Tufts University.



> continued on page 2

in the next issue

Web Security Product Round-up. What's new and what's working in anti-spyware technology, URL filtering, compliance solutions and more. An ever-growing list of products provide companies with a variety of options to address their Web security needs. The Web Security Report narrows the field to highlight some of the industry's latest and most innovative offerings.

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

SPONSORED BY
IRONPORT SYSTEMS



Unfortunately, spammers and other malware purveyors didn't get the message.

In his newly-released book, *Upping the Anti- In Pursuit of the Accountable Internet* (Messaging Media Press—2007, www.uppingtheanti.com), author Tom Gillis reports that spam volumes dropped in the first half of the decade to manageable levels through heightened vigilance and the use of more accurate filters. By late 2006, however, they more than doubled, demoralizing network and IT

administrators around the world. The spike in this bad traffic reflects the considerable money to be had as a big time spammer, and the aggressive tactics these perpetrators now deploy.

The actual composition of spam changed significantly from 2005 to 2006—with the percent of spam containing easily blockable URLs falling by nearly half, and the use of text- and image-based spam rising dramatically.

"It's a problem that has gotten out of control," Gillis said in an interview prior to the release of *Upping the Anti-*. "That's because there is a lot of money at stake. If you look at its evolution, the core reason why spam has managed to exist is because the people who send it don't bear any of the costs. It's becoming so difficult to trace that there's virtually no accountability."

Meanwhile, the threats and associated costs for enterprise networks and Internet Service Providers (ISPs) are growing as security professionals scramble to meet these expanding challenges.

"The way we have attacked the problem of spam, viruses and spyware has been through filtering on the receiving side," said Gillis, the Chief Marketing Officer of IronPort Systems, who also authored *Get the Message – A Business Guide to Surviving the Email Security Crisis* (Messaging Media Press—2004). "Ultimately that's not sustainable because the senders can just double the volume. That means our filters have to go from 98 percent to 98.5 percent to keep up. That may seem small, but it's a hard jump to make."

Until users address the need for greater accountability on the Internet, Gillis says, email and Web technologies will continue to provide the ideal platform for profit-hungry spammers and malware writers.

How Spammers Got Us in This Mess

In early 2006, just when many thought real progress was at hand, spammers redoubled their efforts to force their messages into as many mailboxes as possible.

In *Upping the Anti-*, Gillis reports that just three years ago most spam was classified as "grey mail" (unsolicited email that advertises legitimate products like mortgages or fabulous vacation packages). In this comparatively naive era, retailers paid spammers on a "per-clickthrough" basis for attracting customers to their offers. Using these affiliates to sell their products, however, provides the retailer with limited control over the way in which sales traffic is generated, leaving the spammers with free reign over how to generate leads. Their methods have often been illicit at best, and outright illegal at worst.

In his latest book, Gillis notes that the actual composition of spam changed significantly from 2005 to 2006—with the percent of spam containing easily blockable URLs falling by nearly half, and the use of text- and image-based spam rising dramatically. This

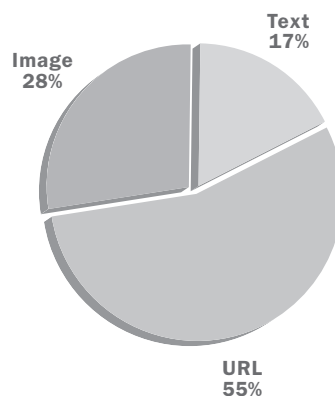


Figure 1: URLs Lead the "Call to Action" in Today's Spam Messages

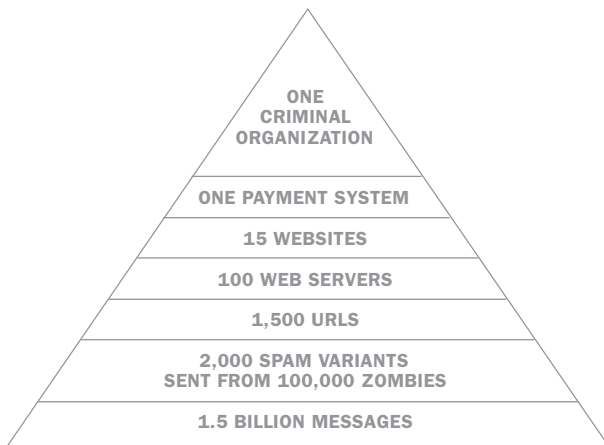


Figure 2: Hierarchy of a Spam Attack

rise in image-based spam is particularly troublesome, as increased message traffic has caused throughput to nearly triple over the last year. As a result, networks are being overwhelmed, backing up message queues and delaying the flow of legitimate email.

Gillis also reports that rapid outbreak spam attacks have also increased as spammers adopt techniques long-deployed by virus writers. In essence, spammers are experimenting with variants to be sent out in limited quantities as a means to test their effectiveness against various filters. Once they hit on an effective strain, they strike with a large-scale and overwhelming attack, which runs rampant until the spam filters determine how to react.

Upping the Anti- cites a jump in 2006 of two specific types of solicitation: stock spam and pharmaceutical spam—which are now the most prevalent. Gillis reveals how stock spammers use their virtually cost-free method of delivery to build up interest in little-known stocks (in which that they have invested). Billions of messages may be sent with the hope that a fraction of a percent of the recipients will bite on the call to buy. Known as “pump and dump,” the intent is to increase the value of the stock—often based on the debatable research analysis included in the spam message—so that investors will purchase the stock and drive up its price. Once the price has risen to a desired level, the spammer/investor can then sell his stake at a profit.

Pharmaceutical scammers are also relying on spam as a means to connect (often illicit) offshore suppliers with consumers. With typical “pharma” sites moving around frequently, this modern day drug trafficking is difficult to detect. In the *Upping the Anti-* “Investigative Report” appendix, Gillis showcases a real world example of how this works (see Figure 2) by deconstructing a complex attack that consisted of more than 1.5 billion messages sent with distribution through more than 100,000 hijacked PC mail servers operating from 119 countries. Roughly 2,000 variants were deployed, changing the spam content every 12 minutes to avoid signature detections, while the URLs used in the spam rotated through 1,500 domains to steer clear of blacklists. These rotating URLs pointed to 100 Web servers for 15 different pharmaceutical sites, each with a unique look and feel, but sharing a common payment processing and customer support system operated by a single entity.

Such a massive and randomized attack, Gillis reports, underscores the complexity and sophistication of today’s spammers, and the increasing reliance on coordinated email and Web-based technology.

The Mounting Threat of Viruses and Spyware

While 2006 saw a decrease in the number of large-scale virus outbreaks, Gillis indicates that the attacks that hit were decidedly more sophisticated and malicious than in previous years.

In *Upping the Anti-*, he reports a significant rise in URL-based viruses, which spread via email. These damaging, Web-borne messages are relatively simple—containing only a subject line, a URL and no attachments. As such, they can be easily scanned and their legitimate appearance makes it extremely difficult for traditional security systems to stop them.

Gillis also notes the recent rise in macro-based viruses, which reside within Microsoft Office program files. These viruses attack under the radar by capitalizing on email administrators’ current reliance on attach-

————— > *continued on page 4*

ment scanning techniques. The viruses capitalize on users' familiarity with file types such as Word and Excel for higher open and infection rates.

He further predicts a significant increase in the volume of viruses carrying spyware payloads. Spyware has continued to rise in the past year. In a recent analysis, The IronPort Threat Operations Center reported that nearly one half of all corporate PCs were infected with malware, including adware, tracking cookies, Trojans and system monitors. This rate of infection is remarkably high, writes Gillis, given that 65 percent of the enterprises who participated in this study reported that they deployed some type of desktop-based, anti-spyware system.

Today's spyware generators succeed through site poisonings and site spamming. As Gillis explains, site poisoning involves the secret delivery of spyware through links to legitimate, high-traffic websites. This can be achieved by hacking into the site, frequently by tricking vulnerable browsers into downloading the malware. More recently, sites can be poisoned through linked content. This can be achieved when a site pulls content and code from another site. This is common when one site references another site, and is often set up through an advertisement.

In *Upping the Anti-*, Gillis presents a classic example of site poisoning in the case of MySpace.com, which inadvertently delivered malware through an ad it served. In this case, the ad attempted to download a Windows metafile (.wmf) image, which could transmit and download malicious code by exploiting vulnerability in the Internet Explorer browser. This provided a critical opening for the secret distribution of adware to unsuspecting end-users. The example highlights the need for legitimate sites to better control content from external sites that can be passed on to their visitors

Site spamming refers to the new tactic of spyware writers and distributors: creating fake sites that are specifically designed to take advantage of browser vulnerability and spread malware. *Upping the Anti-* details how traffic is driven using spam or phishing email messages containing URLs that point readers

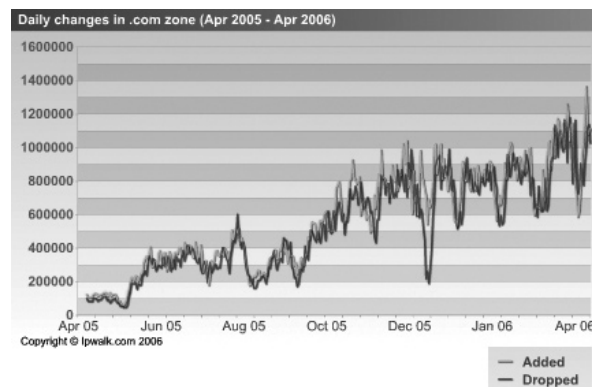


Figure 3: Spammers Register and then Drop Spam URLs within Hours, Making Accountability Nearly Impossible (Source: www.ipwalk.com)

to these nefarious sites, which have been creatively crafted to appear legitimate. This blend of email and Web technology underscores the frightening coordination and capabilities of today's malware writers.

Winning the Battle: How We Get There From Here

According to *Upping the Anti-* the latest trends in spam, viruses and spyware, "paint a grim picture." Gillis writes that, "The power of the profit motive appears to be propelling these threats faster than the technology to counter them can be deployed." Indeed, the book warns that simply providing new filtration solutions designed to meet these threats on an ad hoc basis can no longer keep pace with the ability of malware to mutate and circumvent such defenses.

The lack of accountability on the Internet rests at the heart of this problem. Consider that a spammer can send spam from a hijacked PC, and (within seconds) switch to another different one. The chance of tracking this criminal down and holding him responsible is virtually non-existent. The only hope for bringing accountability to the Internet, concludes Gillis, is a fundamental shift in the way email and the Web work.

"Right now, the situation is pretty lawless," Gillis said in a recent interview. "We have to change the way the Internet works to achieve accountability."

“When you send a physical letter, the letter is registered, in effect, with a return address and a postmark. In telephony, calls can be traced back directly to the caller. This isn’t the case with spammers and the like, who can simply shed their skin to avoid detection and liability.”

Without accountability, Gillis warns of continued erosion of trust in the Internet. To restore lost trust and avoid the direct and indirect costs of fighting spam and malware, *Upping the Anti-* offers a collection of solutions that address Web and email abuse. The answers, he contends, rest in advancements in reputation- and identity-based analysis as well as more meaningful policy development and enforcement.

The Web Strategy: Addressing the ‘Big Head and Long Tail’ Problem

Prevailing Web-based attacks via site spamming and site poisoning demand strategic rethinking of existing security solutions. The pull-based nature of the Web makes reputation analysis the most appropriate security approach. First generation Web security relied heavily on URL blacklists—whereby, if a site was determined to contain spyware, it would be added to a list of bad IP addresses and blocked. In theory, this is a smart approach. In practice, however, it is too reactive—relying heavily on human experience to classify threats. Today’s rapid proliferation of pirate sites, which can come and go in a day, demands a more proactive method of defense. The reality is that malware thrives on obscure, low-volume sites. Gillis notes that this reflects what is known as the “big head, long tail” feature of the Internet. A comparatively small number of large, legitimate sites comprise the big head, while smaller, sometimes bogus sites account for the long tail. Tracking the reputation of sites in this long tail is a daunting task.

Modern reputation systems obtain their first information on a site from domain registrars. This

useful knowledge triggers initial reputation scoring through critical analysis of the site’s country of origin, DNS server configuration and the server’s IP range. However, this is only a first line of defense, and Gillis advocates that it be coordinated with an application-layer server. Deployed with a security system at the application level, a network-level reputation system can pose a serious obstacle for malware authors.

Gillis also contends that more rigorous domain registration is required to prevent pirate malware or spam sites from easily registering new domains, which are frequently established, operated as rogue sites and discarded within 24 hours, with no accountability or cost (see Figure 3). Requiring registrants to validate a new domain with a credit card or address before allowing their sites to be turned on would provide an excellent deterrent. To further diminish site poisoning, Gillis suggests that owners of the legitimate sites be more vigilant in ensuring the content of their sites—using banks of scanners to analyze incoming content.

Prevailing Web-based attacks via site spamming and site poisoning demand strategic rethinking of existing security solutions. The pull-based nature of the Web makes reputation analysis the most appropriate security approach.

Fixing Email

Not long ago, spammers worked around industry blacklists by exploiting the open relay function built into SMTP. This enabled them to send messages that could only be traced to the legitimate IP address of the relaying mail transfer agent (MTA). Ultimately, blacklists began to target open relays by employing the Open Relay DataBase (formerly located at: ORDB.org) to track the servers that allowed such unrestricted traffic. While some legitimate mail was lost in the process, the end result has been a decrease in open relays.

Spammers, however, have found new ways to mask their identities. Looking to the success of virus writers, spammers developed ways to infect PCs in a manner

————— > *continued on page 6*

that enables them to continue sending mail to the Internet. These infected computers are known as “zombies”. A large collection of zombies, controlled by a third-party spammer, is known as a “botnet.” Most zombies are part of consumer broadband networks, which serve millions of subscribers using dynamically assigned IP addresses. Zombies are the ideal conduits for spammers because of the fact that, when a PC connects to the Internet, it is assigned an IP address for the duration of its session. Consequently, a zombie PC assumes a new identity each time it connects. For spammers, this is the equivalent of having a new Social Security number at their disposal every few hours.

Gillis warns that the IT community will need to work harder at outbound traffic filtering if it hopes to preserve the reputation of legitimate messaging.

In this dynamic environment, simply categorizing specific IP addresses as dangerous would end up blocking far too much legitimate mail. Reputation-based

tracking, therefore, provides the best opportunity for dealing with spam-sending zombies. Today’s modern granular reputation systems are able to recognize a new sender coming in from a server in a dynamic IP range. While this does not provide the basis for blocking, it does inform and alert the recipient that this mail should be treated with caution.

Throttling (limiting the rate of delivery) of suspicious mail, also provides recipients with an effective tool for determining whether the content of questionable senders’ messages is legitimate. Gillis notes that this system relies on reputation monitoring at the network level, and content scanning at the application level, and is the basis for IronPort Systems’ gateway security products.

As spammers react to such defense tactics as resources to identify open relays and widespread reputation filtering, Gillis anticipates that they will turn to a new generation of zombies, which will transfer their messages through legitimate ISPs or corporate MTAs (rather than directly onto the Internet). This will have a significant impact on the reputation and deliverability of legitimate mailers.

Gillis warns that the IT community will need to work harder at outbound traffic filtering if it hopes to preserve the reputation of legitimate messaging. This will be particularly difficult for ISPs, which handle large volumes of mail. To secure their reputation as honest mail deliverers, ISPs will be required to make significant investments in their networks.

In the meantime, domain-level authentication provides a promising tool for enterprise and ISP administrators. DomainKeys Identified Mail (DKIM) has emerged as an excellent resource for ensuring Internet accountability. Relying on proven cryptographic techniques to validate the domain that appears in the “Mail from” header, DKIM essentially places an invisible digital stamp of authenticity, which can be easily recognized by receiving mail servers. DKIM enables recipients to verify that the message

DKIM Defined

The DomainKeys specification, designed by Mark Delany of Yahoo!, has adopted aspects of Identified Internet Mail to create an enhanced protocol called DomainKeys Identified Mail (DKIM). This merged specification is the basis for an IETF Working Group that plans to guide the specification toward becoming an IETF standard. A list of organizations supporting DKIM include:

Alt-N Technologies	iiNet LTD
AOL	IronPort Systems
Apache SpamAssassin	MailFrontier
Brandenburg Internetnetworking	messagesystems
CipherTrust	Mirapoint
Cisco	PGP Corporation
Cox Communications, Inc.	Port25
EarthLink	gmail.org
EBay/PayPal	Sendmail
eleven GmbH	StrongMail Systems
Epsilon Interactive	Trend Micro, Inc.
Habeas	Tumbleweed
IBM	Verisign
Iconix	Word to the Wise
	Yahoo!



To ensure accountability, and allow accurate flow of information, mechanisms such as identity, policy and reputation must become part of the network infrastructure.

came from the domain it specifies—even if it went through multiple hops in the forwarding process. DKIM’s popularity, Gillis says, can be credited to its immediate benefit as the viable solution to fraudulent “phishing” emails. DKIM also provides a mechanism for analyzing the domain reputation of a sender from a dynamic IP. Identifying a domain-based reputation is particularly useful in stopping zombies, because the process does not rely on an IP address, which can change frequently and arbitrarily.

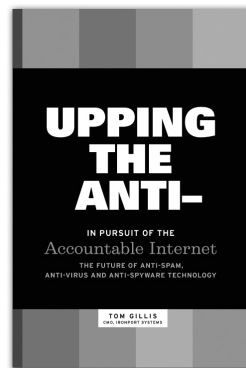
Gillis also looks to the examination of “received headers” as a strong means of bringing greater accountability to the Internet. Under current SMTP protocol, email accepted by an MTA and transferred to the Internet is stamped by the MTA with the IP address of the server that submitted it. This stamp is known as the “received header.”

Closer analyses of received headers offers a viable means of fighting spam because it is relatively easy to distinguish legitimate mail that is passed from a designated server through a designated MTA from the very different received headers that would be seen in messages emanating from a zombie PC. However, the lack of a standard format for inserting received headers makes them difficult to read and interpret. They can also be easily forged. “In the

accountable Internet,” Gillis writes, “a sending MTA should take responsibility for verifying the received header of an email in the same manner in which a local post office is responsible for putting an accurate postmark on a message.”

Gillis concludes that the best way to enforce and ensure Internet accountability lies in the ability to tie reputation through a means of identification that reaches all the way back to an individual desktop. So, if a machine is infected, its reputation as a sender will suffer. Such a solution would require a dramatic change that could take years to develop. The key, he notes, is that conversations to achieve that vision begin today.

“We must keep exploring the solutions with full appreciation for all the valid privacy issues out there, but also with a real understanding of the costs now being incurred and that will grow if spam and spyware aren’t stopped,” Gillis said. “We have to begin tying this bad behavior back to the individuals if we hope to bring real accountability back to the Internet.”



Free copies of Gillis’ new book, *Upping the Anti-*, are available online at: www.uppingtheanti.com.

About the Author

Paul Gargaro is a freelance writer whose work has appeared in such publications as *The New York Times* and *Detroit Monthly*. He has held staff positions with *The Bridgeport Post*, *Crain’s Detroit Business* and *Bloomberg News*.

SEC Halts Trading on Spam Driven Stocks

The U.S. Securities and Exchange Commission (SEC) recently announced that the agency had suspended trading in the securities of 35 companies, each of which has had its stock price significantly manipulated by spam email campaigns. The agency's retaliation, dubbed "Operation Spamalot", aims to reduce the viability of such scams by blocking trading in the companies touted via email bombardment.

The companies themselves are usually unconnected to the spammers. Although the trading suspension only lasted ten days, the SEC pledged to continue its investigation into the spam campaigns until the perpetrators are brought to justice.

For the full SEC press release, visit: <http://www.sec.gov/news/press/2007/2007-34.htm>

Read RSS, Get Hacked

Users of Web feed services, such as Real Simple Syndication (RSS) and Atom, might want to make doubly sure they are not downloading malicious code along with their favorite Web content. The growing use of Web feed readers and the proliferation of content aggregation sites are giving hackers a very simple way to deliver malware onto their computers, analysts warn. Feed readers assume that the content being pulled in is a story or a blog, and make little attempt to sanitize the content. The security problem arises from the fact that many RSS- and Atom-based

feed readers and aggregators simply pull in the content from the source without first checking to see whether it might contain malicious code. Given the number of RSS readers being downloaded every day, and the number of websites that aggregate and publish RSS feeds, it's easy to see why feed injection could become an even bigger nuisance than spam.

Additional information about this story can be found at: http://www.darkreading.com/document.asp?doc_id=118039

E-health Records Don't Have to Threaten Privacy

According to a Harris Interactive Inc. survey, electronic health records can be recorded and shared without jeopardizing privacy. The survey, which was conducted in January, was designed with Alan Westin, a professor of public law and government at Columbia University who studies electronic health records. In the survey of 2,337 adults, 63 percent of respondents said that a move to electronic health records could be done without endangering their privacy, while 25 percent disagreed. In addition, 60 percent of those surveyed said that existing state and federal health

privacy laws provide a "reasonable level" of privacy. The survey comes at a time when privacy concerns are at the forefront of federal government and health care providers' efforts to help spur the adoption of electronic medical records and the creation of nationwide networks to share them.

To view the full details of the survey and its findings, visit: http://www.harrisinteractive.com/harris_poll/index.asp?PID=743

Initiative to Test Secure Coding Skill

A coalition of security companies and organizations recently announced a plan to create assessment tests that would certify programmers' knowledge of secure coding practices. The groups, led by the SANS Institute, aim to create a set of four tests covering major programming languages that could give companies a tool to measure software developers' ability to create secure code. The tests would also

act as a guide to software buyers of the ability of developers, as well as giving coders a way to identify gaps in their knowledge. The exams will be piloted in August in Washington D.C. and then rolled out worldwide during the remainder of 2007.

Full details are available at:
http://www.sans-ssi.org/ssi_press.pdf

Online Pharmacies Can Be Deadly

Think those spam messages and webpages touting deeply discounted drugs are a great deal? Believe the latest link is too good to pass up, the message too compelling to ignore? Just remember: buyer beware. Following the death of a 57-year old Canadian woman, computer users are being cautioned on the dangers of buying pills from online sites. Marcia Bergeron died of poisoning after taking pills (labeled as anti-anxiety medication and sedatives) purchased from a purported Canadian Internet pharmacy, which used fake endorsements from medical agencies. The coroner's report revealed that the counterfeit

pills contained dangerous levels of the heavy metals strontium, uranium and lead. An inquest, which will include an investigation into Bergeron's computer, may uncover additional details. Experts express concern that more deaths may occur among patrons of online "pharma" sites—such as the one from which Bergeron bought her medication—warning that these sites are growing in both danger and number.

To learn more about this story, visit: <http://www.medadnews.com/News/index.cfm?articleid=425998>

company spotlight

Entrust, Inc.

Entrust, Inc. is a world-leader in securing digital identities and information. Over 1,500 enterprises and government agencies in more than 50 countries rely on Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. The company's proven software and services help customers achieve regulatory and corporate compliance, while turning security challenges

such as identity theft and email security into business opportunities. Headquartered in Dallas, TX, the company also offers services such as consulting, deployment and managed security. www.entrust.com

The Entrust logo is displayed in a white rounded rectangle. The word "Entrust" is written in a bold, dark blue, sans-serif font.

IRONPORT SYSTEMS, the leader in Internet Gateway Security, has developed 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 is now the industry's first and only Web security appliance to combine URL filtering, reputation filtering and anti-malware filtering on a single, integrated platform. By combining these innovative technologies, the IronPort S-Series allows organizations to address the growing challenges posed by securing and controlling Web traffic.

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 a corporate network—allowing IT administrators to proactively and efficiently launch desktop clean up efforts.

Application-Layer Processing

The IronPort S-Series also includes an extremely high-performance Web proxy, along with integrated caching and content acceleration capabilities. 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. Being a Web proxy allows for comprehensive content inspection at the application layer — a critical requirement for ensuring accuracy against Web-based malware.

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. This combination of intelligent scanning and streaming of data yields a decrease in latency that approaches 1/10th that of traditional ICAP-based signature scanning systems — making the IronPort S-Series imperceptible to end-users.

By combining the DVS engine with best of breed signatures, the IronPort S-Series protects organizations against the broadest range of Web-based malware. The IronPort Anti-Malware System™ quickly and accurately detects and blocks a full range of known and emerging threats, including adware, Trojans, system monitors, keyloggers, rootkits, malicious/tracking cookies, browser hijackers, browser helper objects, phishing and more.

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 IronPort Web reputation system can make a very accurate determination



The IronPort S-Series Web security appliance: an industry-leading solution for securing and controlling Web traffic.

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

By assigning a reputation score, and using that input to make scanning decisions, IronPort Web Reputation Filters™ maximize system throughput, reduce latency and increase overall accuracy by as much as 20 percent.

Integrated URL Filters

IronPort URL Filters™ include one of the industry's largest databases to address acceptable use policy concerns incurred due to Web traffic usage. With over 50 categories, approximately 20 million sites covered (corresponding to over 3 billion webpages) and global coverage across 70 languages and 200 countries, IronPort URL Filters offer the broadest reach and the highest accuracy rate in filtering Web content. With automatic daily updates and more than 100,000 new sites being added on a weekly basis, enterprises can rest assured that their policies are always applied against the most current rules.

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.

IronPort S-Series appliances include a flexible policy control platform called IronPort Web Security Manager™ which unifies policy creation for all filtering services on the appliance and provides granular options for the Enterprise based on authenticated or non-authenticated users in their network.

Along with flexible policy creation tools, every IronPort S-Series appliance comes with IronPort Web Security Monitor™ — a real-time threat monitoring and reporting system. The system tracks all network traffic to provide a single location from which to monitor acceptable use policy violations and a broad range of Web security threats. This provides security officers and administrators with comprehensive visibility and actionable insight into their Web traffic infrastructure.

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 unique 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 Web or email messaging system, visit www.ironport.com or call 650-989-6530.



www.ironport.com

**PAGE 1 Can We Make the Internet Accountable?
Only If We Up The "Anti-"**

A profile of author and industry expert, Tom Gillis, and his new book: *Upping the Anti-In Pursuit of the Accountable Internet*. Spam, viruses and spyware are tearing apart the very foundation of the Internet. *Upping the Anti-* explains how these problems came to be, and how they must be addressed.

PAGE 8 Web Security News

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

PAGE 10 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