

INTERNET SECURITY TRENDS FOR 2007

A REPORT ON SPAM,
VIRUSES AND SPYWARE

BY TOM GILLIS

Table of Contents

Introduction	3
Technological Innovation by Criminals: Money and Mayhem	5
Spam Trends	7
Investigative Report.....	9
Virus Trends	13
Spyware Trends.....	17
Winning the Fight with Best Practices	21
Conclusion	23

DURING A SPEECH AT
COMDEX IN 2004,
BILL GATES
PREDICTED THAT...

“the spam problem
would be eliminated.”

SPAM IS
BACK

Introduction

The year 2006 was extremely active for messaging security. Most notably, spam is back. During a speech at Comdex in 2004, Bill Gates predicted that the “spam problem would be eliminated.” In 2005, industry analysts and pundits observed a marked decrease in the growth rate of spam, and some major networks such as AOL even reported a modest decrease in spam volumes. Spam filter efficacy was high enough worldwide that many end-users might have agreed with Mr. Gates’s pronouncement that the spam problem was solved. But in the final months of 2005, the spammers returned with a vengeance. Spam volumes surged in the second and fourth quarters, causing a 200 percent increase in spam volume for the year. Most of this volume increase was driven by advanced image-based spam, which is very effective at evading first-generation filters. Image-based spam is typically 10 times more prevalent than text spam, so the resulting mail throughput (measured in Mbps) more than tripled in 2006—meaning that email gateways around the world needed 300 percent more capacity in 2006 than they did in 2005. And this surge continues. In 2007, spam volume will again more than double, and spam throughput is expected to again triple, putting strain on global email infrastructure and causing disruptions in legitimate email delivery.

Viruses are a popular tool used by spammers to facilitate delivery of their messages. In 2006, virus writer tactics shifted, while 2004 and 2005 were marked by massive outbreaks that created front-page news. The problem with these attacks is that they created such notoriety that it inhibited their effectiveness. In 2006, the frequency and size of outbreaks decreased, but the sophistication and maliciousness increased. Instead of using exotic attachment types that could be fairly easily blocked, virus writers began embedding harmful executables in common business file types such as Microsoft Word and Excel files. Also, virus writers introduced new, highly polymorphic viruses that created many variants in a short time, thwarting the efforts of signature vendors.

Spyware and other Web-based malware attacks also flourished in 2006. Two major tactical shifts were observed in malware delivery during the year. The first was the increase in “site poisoning,” in which malware designers find ways to embed their malicious code into otherwise legitimate sites. The infection of MySpace.com, which resulted in the infection of millions of consumer PCs, was a high-profile example. The second tactical shift was the introduction of “site spamming,” in which malware authors create sites designed to distribute malware, and then drive traffic to those sites using spam and phishing techniques. An excellent example of this tactic was the activity surrounding the VML exploit, where massive spam attacks drove users to malware-infected sites. This demonstrated the sophisticated use of blended threats that combine email and Web technologies in a coordinated attack.

“FIGHTING SPAM

will continue to be

a top priority in

2007.”

—THE RADICATI GROUP

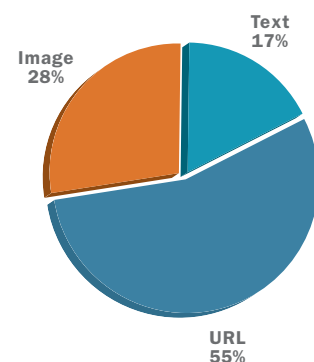
Technological Innovation by Criminals: Money and Mayhem

The reason that Bill Gates and others have grossly underestimated the growth of spam, viruses and other threats is that they have underestimated the motivation of the perpetrators. In 2006, the bad guys got a business plan and deployed enormous amounts of technical resources—designing and executing highly organized global networks to carry out spam, virus and spyware attacks. Adam Smith, the 18th-century economist, brilliantly described the forces of capitalism as an invisible hand guiding individuals to collectively make optimal choices that would benefit society as a whole. True to Smith's predictions, the power of profit has fueled remarkable innovation in malware creation and delivery; however, since the perpetrators don't bear the full cost of their actions, malware is a problem that appears unbounded. Spam volumes have doubled and tripled annually, with no end in sight. The result is that the costs of this increased volume are borne by email receivers, not spammers.

The profits come in a variety of forms. In 2004 and 2005, the majority of spam was "grey mail"—unsolicited email that actually advertised legitimate products such as low-interest mortgages, herbal remedies and ergonomic mice. The retailers then pay spammers on a "per-clickthrough" basis for attracting customers to these legitimate offers. Many legitimate and well-known brands sell products online using an "affiliate" model—by which the retailer pays the affiliate for traffic, but has little control over how the affiliate generates this traffic. Thus, spammers get paid real money for generating real leads by using illicit (or outright illegal) spam techniques.

In 2006, this mix shifted significantly. Stock spam surged from less than 10 percent of spam in 2005 to more than 30 percent of spam in 2006. The result is that both pharmaceutical spam and stock spam are now neck and neck for the most widely sent type of spam today.

The "call to action" in spam messages also changed. In 2005, 85 percent of spam contained a URL, while only 10 percent contained text and 5 percent were image-based. In 2006, spam messages shifted and are now 55 percent URL-based, 17 percent text-based and 28 percent image-based.



URLS LEAD THE "CALL TO ACTION"
IN TODAY'S SPAM MESSAGES

Two classes of spam in particular have surged. The first is spam associated with “pump-and-dump” scams (see Figure 1). A spammer will take a position—for example, to purchase a lightly traded stock with a small market capitalization. The spammer will then send out millions of spam emails containing spurious “research” stating that this stock is undervalued and is expected to rise. An example is shown in Figure 1: bogus research promoting Goldmark Industries, a real firm traded under “GDKI.PK”. These spam attacks typically involve a billion messages. Say that only 1 percent of the spam messages make it through spam filters, and only 1 percent of those that make it through are actually read. Of the people who read the spam, perhaps only 1 percent are innocent and gullible enough to actually go to their online trading account to take a chance and buy a few shares. Even with such a low percentage of actual transactions, enough demand for the stock is created to materially move the stock price up. When the stock rises, the spammer sells their holding in Goldmark Industries—making a significant, very easy profit. A German university studied this issue and concluded that “the spammers who buy low-priced stock before sending the emails typically see a return of between 4.9 and 6 percent when they sell.”

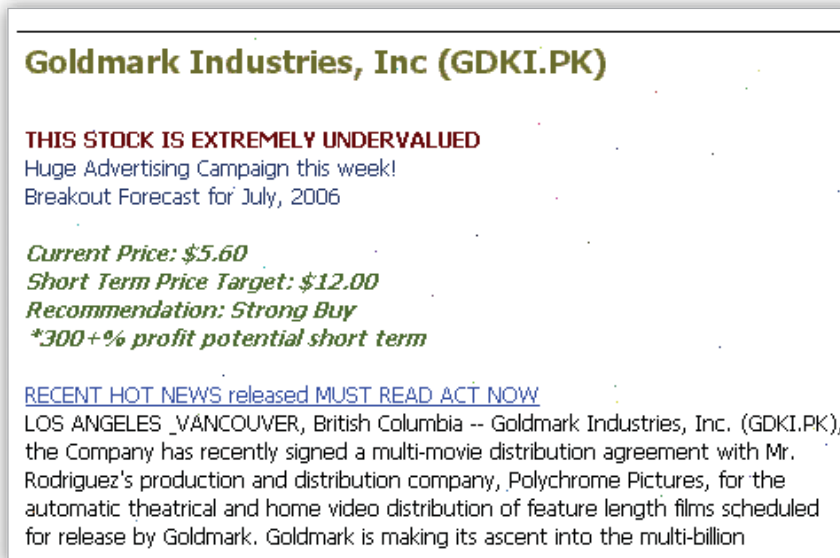


FIGURE 1: PUMP-AND-DUMP SPAM

moved online—along with the sophisticated global organizations that support this crime. Since these “pharma” sites move around frequently, they rely on spam email to attract customers. Pharma spam is fueling much of the growth in spam, as well as the associated viruses and other forms of malware.

The second class of spam that has surged is spam associated with illegal pharmaceuticals. While drug-trafficking is difficult to measure, it is clearly a multibillion-dollar industry. And this industry is loaded with inefficiencies resulting from the many difficulties, most put in place by law enforcement, that separate narcotics suppliers from narcotics consumers. Suddenly, the Internet has created a means to connect illicit offshore narcotics suppliers with a global audience of narcotics consumers. The connection between supplier and consumer is much smoother using online sales, since it is relatively safe for the narcotics consumer and relatively easy for the supplier to avoid detection. Thus, a huge percentage of the drug-trafficking industry has

Spam Trends

As a result of fairly accurate filters and modest volume growth, end-users may have perceived that the spam problem was “solved” in 2005. However, that perception crumbled in 2006 — a year that saw spam volumes more than double. Figure 2 shows this growth of spam message volume.

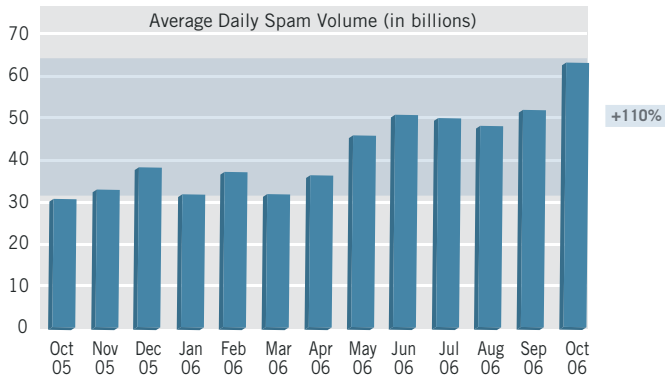


FIGURE 2: SPAM VOLUME DOUBLES IN 12 MONTHS

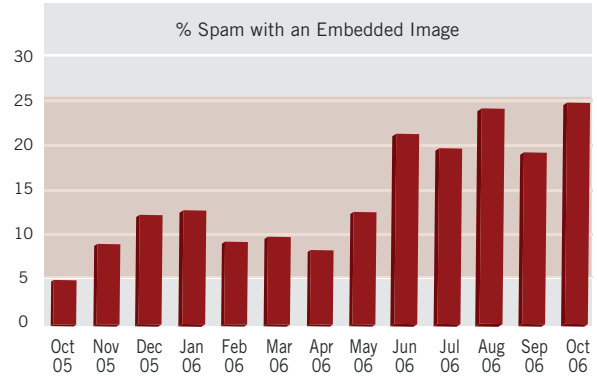


FIGURE 3: IMAGE SPAM DRIVES OVERALL SPAM VOLUME INCREASES

The surges in overall spam volume correlate very strongly with increases in image-based spam, shown in Figure 3.

A typical piece of image spam is about 30 KB, compared with 3 KB for a typical text spam message. This order of magnitude increase in message size has caused spam throughput to roughly triple in the past 12 months. Thus, an enterprise IT staff that had a system running reliably at 33 percent of capacity 12 months ago will find that same system overwhelmed with incoming spam, causing queue backups and major delays in legitimate corporate mail. Figure 4 represents the increase in data volume of spam.

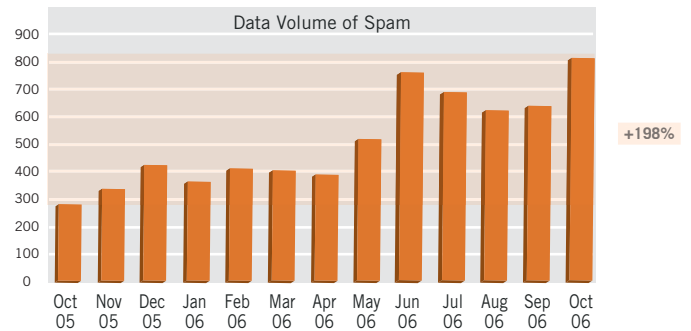


FIGURE 4: THROUGHPUT REQUIRED AT THE MAIL GATEWAY TRIPLED IN 12 MONTHS

Reputation filtering is the best defense against this latest wave of high-volume spam assaults. A state-of-the-art reputation system, such as an IronPort® appliance, can block up to 90 percent of incoming spam at the connection level. Blocking at the connection level ensures that the message is never actually accepted—saving network bandwidth, firewall capacity and email security appliance capacity. While incoming spam data might triple, actual load on a properly tuned IronPort appliance will increase very little.

Another important trend is the increasing frequency of rapid-outbreak spam attacks. Spammers are adopting techniques that virus writers have been using for years. Spammers will develop a new strain or variant of spam. They might send out a very limited trial quantity to see how effective the new strain is against spam filters. Once spammers are confident that they have created a content set that will get through most spam filters, they will launch a very large-scale attack. Figure 5 shows the efficacy of a typical spam filter over time.

The large drop in efficacy, shown in the example on November 16th, occurred during a four-hour window when a new spam attack was launched on a very large scale. Stopping this type of rapid-outbreak spam requires a near-real-time response from a spam filter. Mechanisms must exist to capture samples of missed spam, generate new rules and push these rules out to customers in an automated, efficient manner. Traditional spam filters are inherently reactive, because samples of new spam must be captured and analyzed to create new rules and signatures.

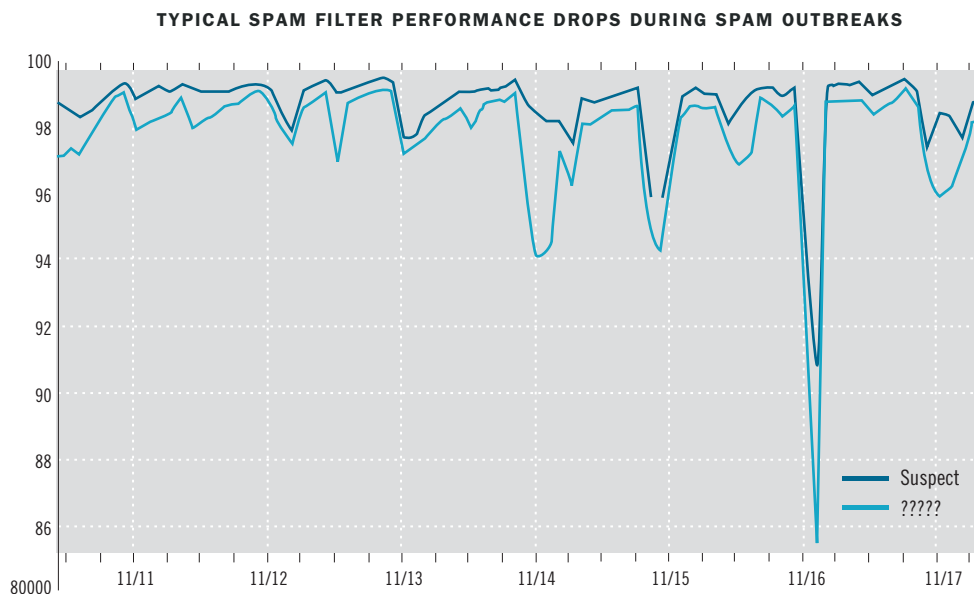


FIGURE 5: THE IMPACT OF A RAPID-OUTBREAK SPAM

A LOOK BEHIND THE CURTAIN AT ORGANIZATIONS THAT SEND SPAM.

Investigative Report

Analysts at the IronPort Threat Operations Center (TOC) recently performed an in-depth analysis of a spam attack, which provided a remarkable view into the scale and global scope of the organizations behind these problems. The IronPort TOC analysts started with a single spam message, offering online medications from www.mithureda.com. A sample of the spam message is shown in Figure 6.

IronPort's threat-clustering technology analyzed billions of spam messages captured by the IronPort SenderBase® Network, and identified the common characteristics that linked billions of seemingly independent and random spam messages into a single, global spam attack. This attack consisted of more than 1.5 billion messages—approximately 5 messages for every man, woman and child in the United States. The spam was sent from more than 100,000 different mail servers, operating from 119 different countries. These spam servers are actually consumer PCs that have been infected by either a virus or spyware and use “zombies” to relay spam. The IronPort TOC analysts found more than 2,000 different variants of this message that could all be correlated to the same spam attack. These 2,000-plus variants were introduced over a two-week period, changing the content of the spam message roughly every 12 minutes to evade signature-based spam filters. Similarly, the URLs used in the spam attacks rotated through 1,500 different domains, a new one roughly every 15 minutes to evade the URL blacklists typically used by traditional spam filters. The thousands of rotating URLs pointed to approximately 100 different Web servers. These machines were serving any one of 15 different websites, each with a unique look and feel, but all with telltale attributes or “fingerprints” that allowed the IronPort TOC analysts to connect them with the same attack. The 15 websites shared a common payment processing and customer support system, operated by a single organization. The total attack of more than 1.5 billion messages was ultimately traced back to a single entity.

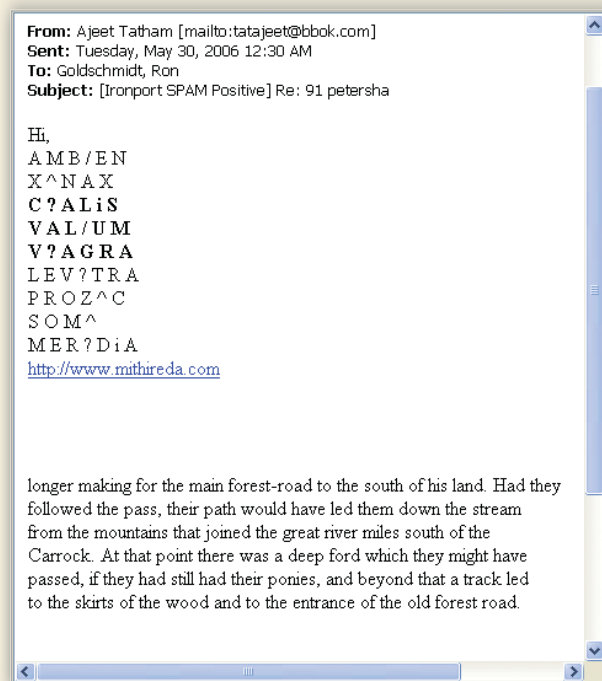


FIGURE 6: “PHARMA” SPAM

Spam attacks of this scale became routine in 2006. Spammers have proved to be very adept at randomizing their messages into thousands of permutations. However, using sophisticated security modeling techniques, the IronPort TOC analysts are able to thwart the attack by identifying and tracking the command and control infrastructure behind it. A summary of these statistics is shown in Figure 7.

In an effort to better understand the source, the IronPort TOC team then performed a detailed analysis of this particular attack. A sample of two of the websites used is shown in Figure 8.

The websites appear legitimate, and contain remarkable detail and background information.

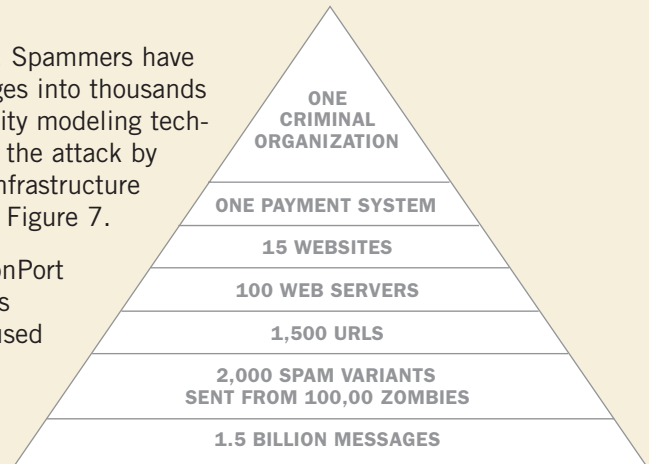


FIGURE 7: HIERARCHY OF A SPAM ATTACK



FIGURE 8: TWO ILLEGAL PHARMA SITES USED IN SPAM ATTACK—VERY DIFFERENT LOOK AND FEEL, SAME INFRASTRUCTURE, SAME SPAMMERS

One of the sites, “My Canadian Pharmacy”, has a long section about the two founders—Canadian doctors who are frustrated by U.S. regulations that deny American citizens access to low-cost pharmaceuticals. These doctors supposedly endeavored to create a site that would provide access to affordable medications for all. The background includes photographs of distinguished-looking doctors and their impressive medical resumés. The website even includes an office address in Canada. However, everything on the website is a forgery. Figure 9 shows a photograph taken at the actual Canadian address—a vacant lot in a rough part of Toronto, next to a sandwich shop.

The website for “My Canadian Pharmacy” was actually hosted by a firm in California whose address is a Post Office box (number 236), shown in Figure 10. The IronPort TOC analysts researched further and ordered some Viagra tablets from “My Canadian Pharmacy.” The tablets arrived in a plastic bag inside a hand-addressed white envelope. The return address of the envelope (and the postmark) indicated that the tablets had actually been sent from an apartment in Mumbai, India—near a pharmaceuticals plant with a reputation for producing knock-off drugs. A photo of the address in India is shown in Figure 11.



FIGURE 9: PHOTO OF PURPORTED ADDRESS OF “MY CANADIAN PHARMACY” HEADQUARTERS

FIGURE 10: THE CALIFORNIA ADDRESS OF THE WEB HOST FOR “MY CANADIAN PHARMACY”

FIGURE 11: THE ACTUAL SOURCE OF THE PILLS FROM “MY CANADIAN PHARMACY”—A RESIDENTIAL APARTMENT IN MUMBAI, INDIA

FIGURE 12: THE ACTUAL TABLETS—TESTED TO CONTAIN PILL BINDER, NOT VIAGRA

The actual tablets are shown in Figure 12. Lab test results showed the tablets have the correct shape, color and markings of Viagra, but contain only inert pill binder. No Viagra exists in these pills.

In summary, this case study shows that a typical spam attack now involves billions of messages using very sophisticated randomization techniques. Spammers have established a very elaborate infrastructure that spans the globe—with spam, in this case, delivered from 100,000 different servers in 119 different countries, and websites and operations that weave through Canada, California and India. The global reach and technical sophistication of this case illustrates how highly organized the entities that create spam have become. IronPort TOC analysts believe that the majority of new, sophisticated spam is coming from highly professional groups with strong links to organized crime. This case also reveals how much reliance spammers place on both email and Web technology to complete these transactions. A coordinated system, which combines both SMTP and HTTP defenses, will yield the maximum protection against these threats. The SMTP system filters mail by looking for spam identifiers as well as dangerous URLs. The HTTP system can also scan for illicit URLs (that might have made it through the spam filter, but that can be blocked on the way out). Additionally, the HTTP system can ensure that any traffic to the suspect sites does not include spyware or malware executables.

Behind the Scenes

AN INFINITE SUPPLY OF ZOMBIES

Spammers use infected PCs, or “zombies,” to obfuscate the IP address of the server sending spam. This technique is very effective for avoiding traditional blacklists, and it keeps spam delivery costs near zero. Since more than 80 percent of spam is sent from zombies, many ISPs have attempted to control the spread of infection. But this task is very difficult. Nearly every PC has some level of virus vulnerability. And these viruses are primarily designed to create new zombie networks. Most of the new zombies have been found in nations that are just rolling out their broadband networks, have large populations of old and unprotected PCs and therefore have the greatest virus vulnerability. Figure 13 shows a graph of the geographic distribution of zombies used in a single large-scale spam attack.

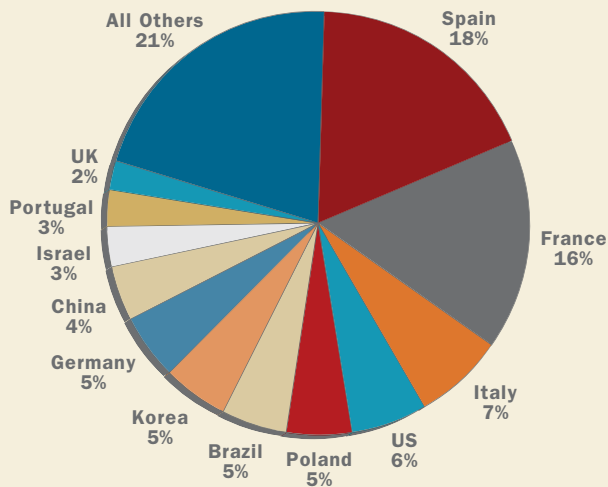


FIGURE 13: A SINGLE SPAM ATTACK USES ZOMBIES FROM MORE THAN 100 DIFFERENT COUNTRIES

HIT-AND-RUN ZOMBIE ATTACKS

The average life span of a zombie in 2006 was less than 30 days. Spammers will make extensive use of a zombie for a few days, until it becomes widely detected and blocked by traditional spam filters. Most traditional spam filters take days to react and

update their rules to block a zombie. By then, the spammer has moved on to another fresh, new zombie. The distribution is shown in Figure 14.

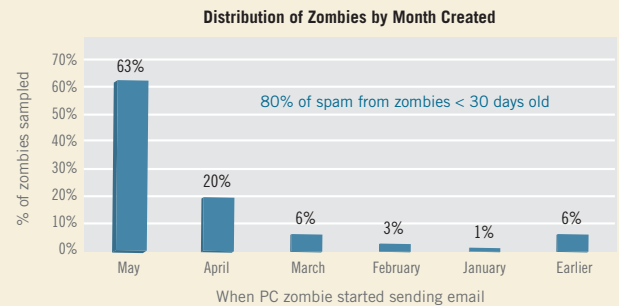


FIGURE 14: MOST ZOMBIES LAST LESS THAN 30 DAYS

AN INFINITE SUPPLY OF URLS

Spammers rotate through URLs as often as every few hours to avoid detection by traditional URL blacklists. Figure 15 shows a huge spike in the number of new URLs registered, as well as a spike in URLs that were dropped. Spammers often register a URL and then drop it before they even have to pay for its use.



FIGURE 15: SPAMMERS REGISTER AND THEN DROP SPAM URLS WITHIN HOURS (SOURCE: IPWALK.COM)

Virus Trends

Although the Internet experienced fewer large-scale virus outbreaks in 2006, these outbreaks were much more targeted, sophisticated and malicious. The monthly average of new virus outbreaks, including virus variants, dropped from 21 in 2005 to 11 in 2006, a 47 percent decrease. However, several disturbing trends emerged:

URL-BASED VIRUSES URL-based viruses increased from 3 in 2005 to 13 in 2006. URL-based viruses are extremely potent because they propagate via email. The email contains only a URL and a subject line that entices a user to click. It is very difficult for a traditional email security system to detect these messages because they look so legitimate. They do not contain an attachment that traditional email anti-virus systems can scan. Instead, they use social engineering to entice end-users to click the link, thereby delivering the virus payload via the Web. Since more and more companies are deploying sophisticated defenses on Port 25 of their network, virus writers are increasingly turning to Port 80—the HTTP (Web) port—as an easy way into the corporate network.

MACRO-BASED VIRUSES Macro-based viruses increased from zero outbreaks in 2005 to 15 outbreaks in 2006. These viruses reside inside Microsoft files—such as Word and Excel files. These viruses can be dangerously effective, as many email administrators rely on attachment file type filtering to limit exposure to new outbreaks. Furthermore, Word and Excel files are much more familiar to end-users, resulting in higher open and infection rates than more esoteric attachment file types.

EMAIL-BORNE SPYWARE Email-borne spyware continues to flourish. As another example of blended threats, email has become a preferred distribution vector for spyware. Six of the ten largest virus outbreaks contained some form of spyware. Most of this spyware involved Trojans, which open a back door on an infected PC and download very harmful code, such as rootkits. From 2005 through 2006, email-borne spyware increased by more than 200 percent, a pace consistent with spyware growth from 2004 to 2005. Clearly, the widespread prevalence of spyware in viruses supports one of the macro trends highlighted by this report—that these threats are coming from the same sources and that the current tactic for attackers is to blend these email and Web techniques.

MULTIPLE VARIANTS Virus writers are using multiple variants of the same virus to evade signature vendors. A great example of this was the Stration virus

RESPOND FASTER. REDUCE VULNERABILITY.

The best defense for a rapid polymorphic virus is to employ a preventive outbreak control system, before signature-based scanning. IronPort Virus Outbreak Filters™ stopped more than 2.4 million copies of the Stration virus, responding an average of 5 hours and 43 minutes ahead of the fastest signature vendors. The IronPort TOC produced a series of 14 targeted outbreak rules that identified and quarantined the outbreak during the vulnerability window.

of 2006. Between September and November 2006, virus writers released waves of variants of the Stration virus, designed to induce customers to open messages by claiming to be security alerts or updates. Many of these variants contained spam engines that were used to propagate the virus by sending out new copies. Figure 16 shows the early proof-of-concept phase of the virus in September, with volume mushrooming in October during the bulk of the outbreak.

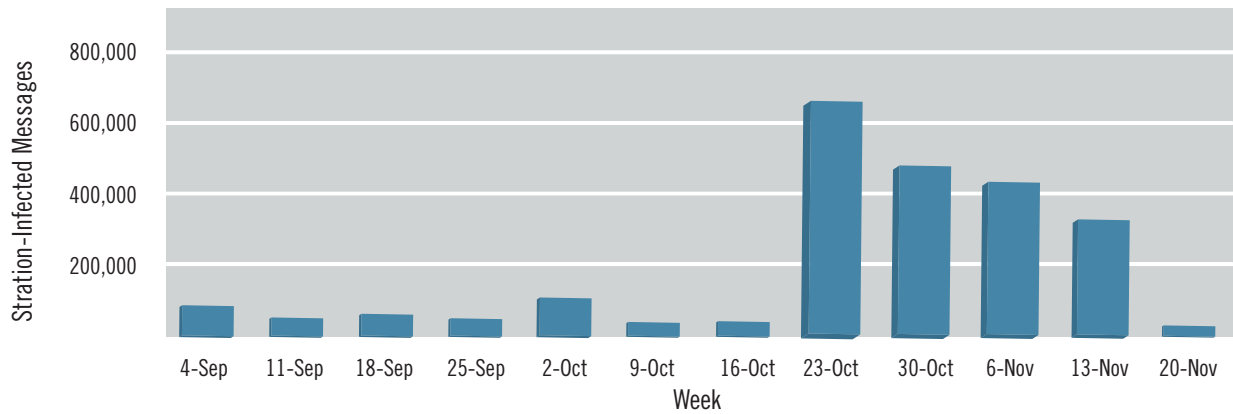


FIGURE 16: THE MANY VARIANTS OF THE STRATION VIRUS FLOWED FOR SEVERAL WEEKS. THE IRONPORT TOC COUNTED 59 SEPARATE MUTATIONS THAT OCCURRED DURING THIS 12-WEEK PERIOD.

The many variants of this virus caused signature vendors long delays in producing signatures, creating significant vulnerability periods for many corporations.

Virus Metrics

IronPort’s TOC saw a slight decrease in the number of virus outbreaks propagating around the world in 2006:

- Analysts observed saw a small increase in the number of virus outbreak rules written during 2006, compared with 2005. In 2005, an average of 70 rules were written each month, for a total of 847. In 2006, the IronPort TOC wrote an average of 74 rules each month, for a total of 888. See Figure 17.
- The number of qualified outbreaks seen by the IronPort TOC remained fairly stable from 2005 to 2006. In 2005, IronPort saw 132 qualified virus

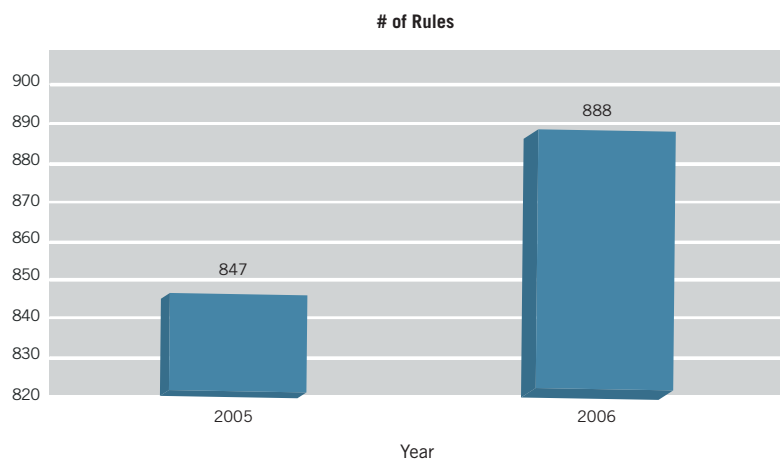


FIGURE 17: NUMBER OF VIRUS OUTBREAK RULES WRITTEN BY IRONPORT’S THREAT OPERATIONS CENTER

outbreaks, for an average of 11 outbreaks per month. In 2006, this number dropped slightly to 123 qualified outbreaks, for an average of 10.2 outbreaks per month. See Figure 18.

- A comparison of the top three virus outbreaks in 2005 and 2006 follows:

2005	2006
Mytob	Stration
Bagle	Bagle
Sober	Mytob

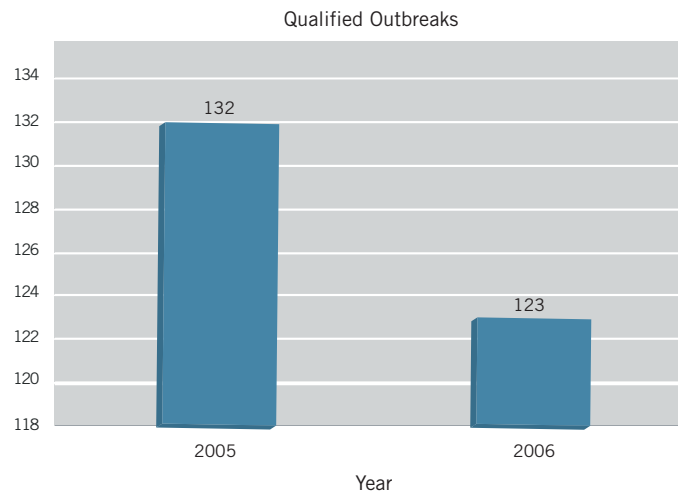


FIGURE 18: NUMBER OF QUALIFIED VIRUS OUTBREAKS AS SEEN BY IRONPORT'S THREAT OPERATIONS CENTER

While it may seem confusing that the number of rules increased while the number of qualified outbreaks decreased, there is an easy explanation. Today's viruses require IronPort's TOC to be more aggressive when writing rules, perhaps duplicating some rules for what turns out to be the same outbreak. A new trend is also emerging. In 2006 the IronPort TOC saw more and more small-scale Trojan attacks (or phishing attacks with a Trojan attached) and less large-scale outbreaks. This equated to less qualified outbreaks. The expectation for 2007 follows the same course. The number of traditional, large-scale, self-replicating virus outbreaks will likely decrease. However, this decline will be negated by the proliferation of smaller, more malicious outbreaks that use URLs and common file types such as Word and Excel to spread. In 2007, an increasing number of viruses will carry spyware payloads. This spyware can enable hackers to take over infected machines, steal personal and confidential information and convert these machines into botnets for use as spam, spyware and virus vectors.

“
WEB-TRAFFIC-BORNE
MENACES LIKE

SPYWARE

are creating an all-time
high concern
among organizations.”

—**BRIAN BURKE**
RESEARCH MANAGER, IDC

Spyware Trends

Spyware continued to spread in 2006. The IronPort TOC staff performed a study of spyware infection rates in corporate environments. This study found that more than 48 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. However, Trojans and system monitors still represented more than 7 percent of the infections, a shockingly high infection rate given the malicious nature of these two types of threats. See Figure 19 for a breakdown.

FIGURE 19: ENTERPRISE MACHINES INFECTED BY MALWARE

Global Infection Rates	Adware	Trojans	System Monitors	Tracking Cookies
Enterprise	48%	7%	5%	77%

These numbers are surprisingly high, given that 65 percent of the same enterprises surveyed had deployed some type of desktop-based, anti-spyware system. Clearly, desktop-based, first-generation malware defenses are not sufficient to protect corporate networks.

Breaking these numbers down by geography gives us the top regions where enterprises are the most infected by malware. Not surprisingly, North America and the United Kingdom hold the top two positions. A detailed breakdown is shown in Figure 20.

FIGURE 20: ENTERPRISE INFECTIONS BY GEOGRAPHY AND MALWARE TYPE

Region	Adware	Trojans	System Monitors	Tracking Cookies
North America	66.7%	9.8%	7.0%	89.4%
UK	46.4%	6.8%	4.8%	74.5%
Germany	43.3%	6.3%	4.5%	69.5%
France	38.7%	5.7%	4.0%	62.1%
Japan	43.4%	6.3%	4.5%	69.7%
China	55.3%	8.1%	5.8%	89.0%
ANZ	39.9%	5.8%	4.1%	64.1%
Other	49.7%	7.3%	5.2%	79.9%

Spyware writers are achieving these infection rates by using two principal tactics:

SITE POISONS The surreptitious delivery of spyware on legitimate websites is known as site poisoning. This tactic can be done in a variety of manners. The brute-force method is to hack into a site and explicitly post malware on it. The malware is typically posted in a manner that takes advantage of a browser vulnerability—tricking the browser into downloading the harmful malware payload.

A newer and more devious problem is site poisoning from linked content. In today's era of Web services, many sites pull content and code from other websites. Often a site may reference another site, which in turn references other sites. RSS feeds and advertisements are frequently set up in this manner. One of the most notable examples of site poisoning was when MySpace.com was found to be delivering malware.

In July 2006, MySpace.com served an ad for “deckoutyourdeck.com”. The ad attempted to download a file called “exp.wmf,” a Windows metafile image. Six months earlier, in January 2006, Microsoft had issued a patch to fix a critical vulnerability in Internet Explorer that allowed .wmf files to cause the browser to download harmful code without prompting the end-user. While the patch had been in existence for nearly six months, the population of unpatched IE browsers was still quite large. Consequently, malware authors were using this exploit to deliver malicious code. This particular exploit attempted to deliver an adware in the Purity Scan family. The ad was served by springfusion.com, a relatively new ad network that claimed no direct responsibility. Controlling content that comes from external sites is an ongoing challenge for legitimate websites.

SITE SPAMMING The second tactic adopted by spyware writers is called site spamming. It involves the creation of bogus sites, designed to deliver malware. Often the site might look legitimate, such as “Mrs. Hall's Second Grade Class,” a fake financial institution or a counterfeit version of a well-known legitimate site such as yahoo.com. A good example of this activity was observed by the IronPort TOC around the VML (Vector Markup Language) exploit in Microsoft Internet Explorer. On September 18, 2006, an IE exploit (that took advantage of the VML vulnerability) was seen in the wild. The exploit forced a buffer overflow in an IE browser and introduced shellcode. If a system was exploited, it allowed the execution of arbitrary code. This vulnerability was observed even in a fully patched Microsoft Windows XP SP2 system.

Initially a proof-of-concept exploit was seen at a few sites that did not distribute any malware packages. As expected, several sites were soon seen hosting this exploit. Exploited systems experienced a significant amount of malware packages, including everything from Trojans, system monitors, and browser hijackers to adware applications. IronPort's own testing of live systems uncovered approximately 30 malware packages coming from just one site. Examples of some of these packages are:

- Trojan-Downloader-AC2
- Trojan-Backdoor-SkyAffiliate
- enBrowser
- Ezula iLookup
- Trojan-Backdoor-Rustock

Sites that were seen hosting the exploit were typically low-volume, relatively obscure adult or gaming sites. IronPort observed a large volume of spam messages that contained URLs pointing to sites known to be hosting the exploit. Two

examples of these spam messages are shown in the following figures. Figure 21 is a phishing email, advertising Commonwealth Bank—an actual Australian bank.

Shortly after the Commonwealth Bank phishing emails, IronPort detected a forged Yahoo! greeting card, shown in Figure 22, that linked to infected sites.

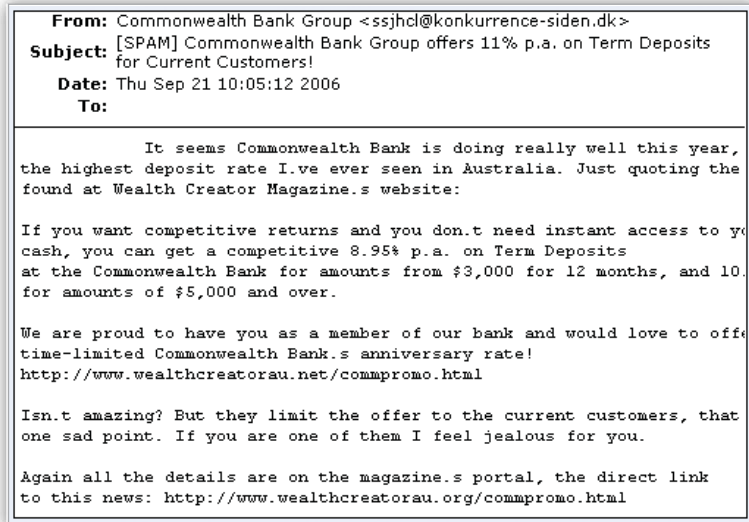


FIGURE 21: PHISHING EMAIL THAT DRIVES TRAFFIC TO A MALWARE SITE

This message is an example of excellent social engineering. End-users would be hard pressed to discover that this is a forgery and would likely click the link and infect their machines.

This site-spamming incident is a perfect example of malware writers using blended threats, email and Web technology to deliver very sophisticated, and very effective, coordinated attacks.

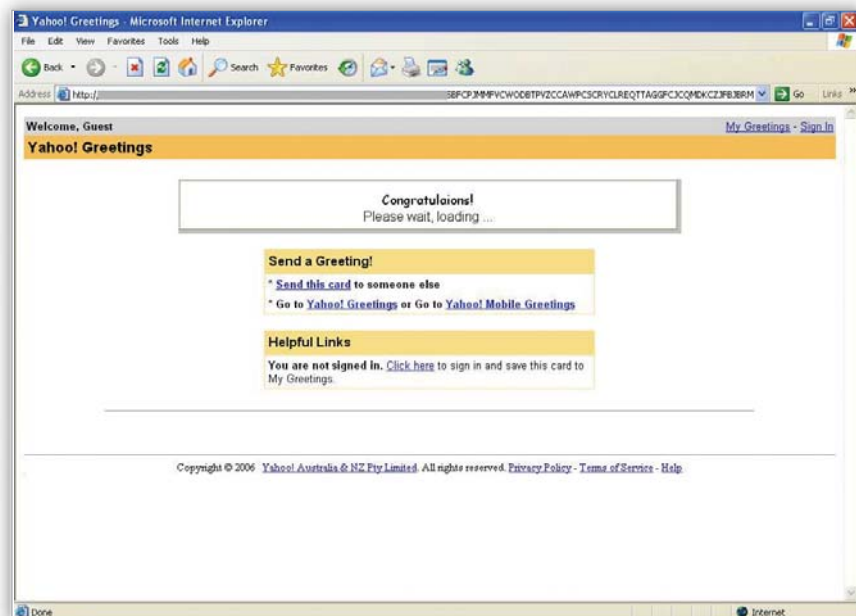


FIGURE 22: A FORGED YAHOO! GREETING CARD DRIVING TRAFFIC TO A MALWARE SITE



IronPort powers and protects your network infrastructure with Web Security, Email Security and Security Management appliances.

WEB SECURITY

The IronPort S-Series™ is the industry's fastest Web security appliance—providing a network perimeter defense for the broadest range of spyware and Web-based malware.

EMAIL SECURITY

The IronPort C-Series™ and IronPort X-Series™ email security appliances are in production at eight of the ten largest ISPs and more than 20 percent of the world's largest enterprises. These industry-leading systems have a demonstrated record of unparalleled performance and reliability.

SECURITY MANAGEMENT

The IronPort M-Series™ security management appliances centralize and consolidate important policy and runtime data, providing administrators and end-users with a single interface for managing their application-specific security systems.

Winning the Fight with Best Practices

There are no silver bullets to eliminate the flaws found in email. The ultimate answer will likely emerge as a mixture of many complementary solutions. The sustained viability of email demands a convergence of market-driven research and technological development with the willingness of email administrators to embrace a new kind of transmission environment—built on adopted best practices, sender identity verification and reputation authentication. The following best practices are just a start in helping organizations begin to reduce the amount of email and Web threats attacking their networks:

CONTROL OUTGOING EMAIL Corporations should block all outgoing mail that doesn't go through one of their SMTP email gateways. This practice allows IT staff to implement policy filtering on outgoing mail and dramatically reduce the spread of viruses and spam from compromised machines.

MANAGE BOUNCES Bounce messages should always be delivered as delayed bounces. Delayed bounces are separate emails sent to the sender that notify him or her of an invalid address. Bouncing messages during the SMTP conversation exposes the corporate directory to spammers looking to harvest valid addresses. Sophisticated commercial solutions have built-in defenses against directory harvest attacks. These defenses stop accepting mail from a given sender if that sender has exceeded a certain number of invalid addresses. This is an important security safeguard.

SEGMENT EMAIL New generations of email gateways are able to place different classes of traffic on different outbound IP addresses. Corporations should use one set of IP addresses for transactional email, another for employee email, and yet another for bounce messages. If any of these various traffic types induce deliverability problems, the IP segmentation contains the damage to only that class of traffic. The best example is the growing instance of spammers sending messages with a bounce address of a known spam trap. If the corporation bounces the message, they end up on a black-list. If the traffic is segmented, then the only thing that gets blocked is the bounce IP—and corporate mail is unaffected.

PROTECT YOUR REPUTATION If your company is doing any email marketing, check with an email reputation service such as IronPort's SenderBase (www.senderbase.org) to measure the complaint rates associated with the marketing mail. Segmenting email traffic (see above) makes it much easier to resolve marketing-generated issues, as opposed to employee-generated issues. Most leading reputation services will have some type of program to provide a report that reflects how major ISPs regard mail from your company's IP addresses.

MANAGE YOUR IDENTITY DomainKeys Identified Mail is a method for email authentication. It offers almost end-to-end integrity from a signing mail transfer agent (MTA) to a verifying MTA. In most cases the signing MTA acts on behalf of the sender, and the verifying MTA acts on behalf of the receiver.

The DomainKeys specification 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.

DEFINE EMAIL POLICIES When defining email policies, make them specific to certain groups within the company. For example, adding a disclaimer footer might be a global action, but scanning for a key word such as “proprietary” or “confidential” will yield very high false positive rates unless it is put into a more fine-grained filter such as “scan all mail from engineering going to these five competitors for the following 20 words: proprietary, confidential, project x, project y, etc.”

DEPLOY A SOLUTION Deploy a preventive security solution and advanced spam filtering technology that uses real-time data to stay ahead of spam and other threats, without inducing false positives.

The future is now. A new generation of applications will convert sending and receiving gateways into efficient check-points, where email will either earn the imprimatur of legitimacy or be cast aside as noncompliant. In other words: those who don't play by the rules, simply won't be allowed to play.

Conclusion

At the highest level, 2006 saw an increase in both the sophistication and the volume of Internet security threats. Spammers created triple the volume of image-based spam. This threat has a dual effect on infrastructure: incoming mail throughput has increased four times faster than Moore's law (the typical increase in server throughput), and at the same time the processing required to detect the more sophisticated spam has also increased by more than 100 percent. The net result is a massive jump in throughput required at the email gateway to keep legitimate email flowing. This jump in required throughput has led to email delays, and a huge increase in spam appearing in mail boxes—prompting many end-users to conclude that “spam is back.”

Virus writers shifted from the mass-mailer tactics of previous years to more stealthy attacks embedded in office documents, and with highly polymorphic outbreaks. Malware writers found new ways to deliver a steadily increasing array of harmful code, such as keyloggers and system monitors.

Internet Explorer vulnerabilities have allowed malware code to propagate undetected by the end-user. Also, malware authors developed effective spam and phishing techniques to drive traffic to infected sites, resulting in desktop infection rates of over 50 percent at corporations worldwide.

Trends point to a single overarching theme. Spam, viruses, phishing and malware are tools used by well-organized global entities that are profiting from a variety of criminal activities including drug trafficking, fraud and identity theft.

To combat these sophisticated threats, enterprise security officers need to evaluate solutions that have strong email and Web capabilities. An email appliance and a Web security gateway that work together and share a common threat database is the best way to defend against the sophisticated new generation of threats on the Internet.

2007 PREDICTIONS

SPAM

In 2007, spam volume (particularly image spam) will again more than double, and bandwidth consumed by spam is expected to again triple. This will put a strain on global email infrastructure and cause disruptions in legitimate email delivery. In addition, email administrators need to pay special attention to the release of Microsoft Vista, which may present additional vulnerabilities to be discovered and exploited.

VIRUS

In 2007 the number of traditional, large-scale, self-replicating virus outbreaks will likely decrease. However, this decline will be negated by the proliferation of smaller, more malicious outbreaks that use URLs and common file types (such as Microsoft Word and Excel) to spread. Additionally, an increasing number of viruses will carry spyware payloads by which hackers can take over infected machines to steal personal and confidential information and convert these zombie machines into botnets for use as spam, spyware and virus vectors.

SPYWARE/MALWARE

In 2007, as sophisticated organized crime groups fund development to generate profit, the malware market will become more commercialized. In addition, organized attacks motivated by political or economic interests will rise—potentially creating homeland security threats.

Despite the social and legal ramifications, legitimate businesses are willing to utilize new methods to increase advertising revenues. Video formats on social networking sites and media download sites will increase malware distribution opportunities.

About the Author

TOM GILLIS is a recognized leader in the dynamically charged and high-growth email and Web security industry, and has in-depth knowledge of the challenges surrounding secure network infrastructure. An influential and frequent conference and panel presenter, Gillis has made invaluable contributions to the Internet community, including the SMTPi framework for secure email. He is also the author of the book *Get the Message*. Gillis has held positions at iBEAM Broadcasting, SGI, and Boston Consulting Group (BCG), and is currently the chief marketing officer for IronPort Systems. He graduated with distinction from Harvard Business School's MBA program. He also graduated magna cum laude with an MSEE from Northwestern University and a BSEE from Tufts University.



IronPort Systems, Inc.

950 Elm Avenue, San Bruno, California 94066 TEL 650.989.6500
FAX 650.989.6543 EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems is the leading email and Web security products provider for organizations ranging from small businesses to the Global 2000. IronPort provides high-performance, easy-to-use and technically innovative products for those faced with the monumental task of managing and protecting their mission-critical networks from Internet threats.

DISCLAIMER: The law in this area changes rapidly and is subject to differing interpretations. It is up to the reader to review the current state of the law with a qualified attorney and other professionals before relying on it. Neither the authors nor IronPort make any guarantees or warranties regarding the outcome of the uses to which this material is put. This paper is provided with the understanding that the authors and IronPort are not engaged in rendering legal or professional services to the reader.

Copyright © 2007 IronPort Systems, Inc. All rights reserved. IronPort and SenderBase are registered trademarks of IronPort Systems, Inc. All other trademarks are the property of IronPort Systems, Inc. or their respective owners. While every effort is made to ensure the information given is accurate, IronPort does not accept liability for any errors or mistakes which may arise. Specifications are subject to change without notice. P/N 451-0306-2 1/07