IBM X-Force® 2010 Trend and Risk Report

March 2011

IBM

Dedication

The IBM X-Force® 2010 Trend and Risk Report is dedicated in memory of our friend and colleague Bryan Williams who passed away during this effort. His knowledge and focus on the changing threat landscape of virtualization is documented in this report. Bryan was a highly valued member of the IBM X-Force team since the early days and his contribution to the team, security and IBM are too numerous to list. He will be greatly missed.

Contributors

Producing the X-Force Trend and Risk Report is a dedication in collaboration across all of IBM. We would like to thank the following individuals for their rapt attention and dedication to the publication of this report.

Contributor	Title
Amrit Williams	Director, Emerging Security Technology
Bryan Williams	X-Force Research and Development, Protection Technologies
Carsten Hagemann	X-Force Software Engineer, Content Security
Colin Bell	Principle Consultant, AppScan OnDemand Services
David Merrill	STSM, IBM Chief Information Security Office, CISA
Dr. Jens Thamm	Database Management Content Security
Harold Moss	Emerging Tech & Cloud Computing Technical Architect
Jay Radcliffe	Senior Threat Analyst, MSS
Jeffrey Palatt	Manager, Emergency Response Services
John Kuhn	Senior Threat Analyst, MSS
Jon Larimer	X-Force Advanced Research, Malware
Leslie Horacek	X-Force Threat Response Manager
Lisa Washburn	Global Product Mgr, IBM Security Services—Threat/Cloud
Marc Noske	Database Administration, Content Security
Mark E. Wallis	Senior Information Developer for IBM Security Solutions
Matthew Ward	Senior Product Manager—Tivoli Security
Michelle Alvarez	Team Lead, MSS Intelligence Center(aka Eagle Eyes)
Mike Warfield	Senior Wizard, X-Force
Ory Segal	Security Products Architect, AppScan Product Manager
Patrick Vandenberg	Manager, Rational Security & Compliance Marketing
Ralf Iffert	Manager X-Force Content Security
Ryan McNulty	IBM Managed Security Services & SQL Querier Extraordinaire
Scott Moore	X-Force Software Developer and X-Force Database Team Lead
Shane Garrett	X-Force Advanced Research
Steven Bade	STSM Security Architect and Strategist
Tom Cross	Manager—X-Force Strategy and Threat Intelligence
Wangui McKelvey	X-Force Marketing Manager

About X-Force

The IBM X-Force® research and development teams study and monitor the latest threat trends including vulnerabilities, exploits and active attacks, viruses and other malware, spam, phishing, and malicious web content. In addition to advising customers and the general public about emerging and critical threats, X-Force also delivers security content to help protect IBM customers from these threats.

Contents
Section I

Contents
Section II, III and IV

Navigating the report

Welcome. This year we have made some helpful improvements to the format and content of the Trend Report. These improvements are aimed at enabling readers to take the findings a step further. We understand that computer and network security is about focusing on awareness of the threat and helping to protect the systems and networks from these threats. But then what? As an organization matures in its stance on computer security and known threats, how can they begin to develop a deeper focus towards improvement?

We asked ourselves that question and determined the answer was to provide to our readers a deeper understanding of what we experience and have learned from the breadth of capabilities that is IBM Security Solutions.

For this report we have divided the content into four sections.

- Threats
- Operating Secure Infrastructure
- Developing Secure Software
- Emerging Trends in Security

We start by talking about the threats that our systems and networks are facing, because we have to begin by understanding the problem we are all working to solve. Once a threat is understood, we can work towards realistic technology controls and educational awareness to help secure our enterprise and systems. In both the **Operating Secure Infrastructure** and **Developing Secure Software** sections we not only discuss threats but provide logical advice on how to help improve or detect those threats in your environment. In the **Emerging Trends in Security** section, we take a forward look into emerging technologies that are pressing into discussions as future business concerns.

We believe this new layout better organizes the material we want to present and helps you the reader focus on what is most important to your organization.

Section I–Threats

In this section we explore topics that comprise "Threats" and describe the attacks aimed at the enterprise that security specialists face. We address the malicious activity observed across the spectrum by IBM and how we go about helping protect networks from those threats. In addition, an update on the latest attack trends as identified by IBM.

Executive overview

The second decade of the twenty first century is underway and technology continues to permeate every aspect of our work and personal lives. At IBM we call this the Smarter Planet and we are continuously helping our customers to take advantage of a world that's more interconnected, intelligent, and instrumented. As much as these innovations can increase our efficiency and ability to instantly connect on a global scale, so too can the risks and dangers of a connected world become more sophisticated and difficult to contain.

To prove the point, the confluence of this innovation recently showed its face in several authoritarian countries, where technology and political activism have united to empower people in sharing a voice and making change on a global scale. More generally, we have seen a rise in hactivism across the globe, where attackers are no longer motivated simply by self-recognition or financial gain, but by political change and protest.

The second half of 2010 also marked a highly visible precedent in the industrial and manufacturing space. The multi-faceted and highly customized Stuxnet worm shook up the SCADA world by proving how security vulnerabilities can cripple a factory or production site. No longer is just e-commerce, personal, or corporate data at risk, but the very infrastructure that powers our factories and energy sector can be exposed for exploitation.

On a smaller scale, mobile devices continue to multiply in the workplace, helping increase the magnitude and complexity of risk in protecting the enterprise. In the emerging trends in security section, we look at several mobile vulnerabilities that may be an indicator of more to come. In the enterprise, and at home, web vulnerabilities targeting the browser continue to dominate the majority of weaknesses, demonstrating the importance of patch compliance and host protection. We discuss an interesting case study of how large complex organizations can benefit from centralized patch management.

In our **advanced persistent threat article,** we look at some of the most sophisticated adversaries our networks have ever faced. These types of low and slow coordinated attacks are often an indicator of highly cohesive and organized groups of attackers who use a variety of sophisticated attack techniques to inch their way into the enterprise.

Not only are attacks changing but so is the very technology that we utilize to carry this traffic. We take a quick look at how networks are scrambling to keep up with technology changes. At the mid-year point, we discussed a shift from IPv4 into IPv6 requirements and in this report, we discuss the oncoming advent of DNSSEC.

2010 was a pivotal year on many counts and has shown that understanding the trends of the security landscape is more critical than ever. IBM continues its dedicated effort to educate, inform, and discuss security topics and emerging trends with the community at large. Preparing organizations to not only understand the emerging threat landscape, but also to better understand the weaknesses of an organization's infrastructure.

2010 Highlights

Threats

Malware and the Malicious web

- IBM Managed Security Services (MSS) saw an upward trend in Trojan botnet activity during 2010. This growth is significant because despite increasing coordinated efforts to shut down botnet activity (as seen with the Mariposa, Bredolab and Waledec botnets), this threat appears to be gaining momentum.
- IBM's data illustrates the dramatic impact of a successful effort in early 2010 to shutdown the Waledac botnet, which resulted in an instantaneous drop off in observed command and control traffic.
- Zeus (also known as Zbot and Kneber), continues to evolve through intrinsic and plugin advances. The Zeus/Zbot family of botnets has been around for many years now and due to its extreme popularity with attackers, there are hundreds, or even thousands, of separate Zeus botnets active at any given time. The Zeus botnet malware is commonly used by attackers to steal banking information from infected computers.
- SQL injection is one of the leading attack vectors because of its simplicity to execute and its scalability to compromise large amounts of web servers across the Internet. There also appears to be a seasonal pattern: during each of the past three years, there has been a globally scaled SQL injection attack some time during the months of May through August.
- Obfuscation, whereby attackers attempt to hide their activities and disguise their programming, continued to increase over 2010 and shows no signs of waning.
- Compromise through PDF exploitation continues to be a favorite among attackers. In late April, a particular spam campaign contained an Adobe Acrobat PDF that used the Launch command to deliver malware. At the peak of the attacks, IBM Managed Security Services (MSS) received more than 85,000 alerts in a single day.
- The SQL Slammer worm first surfaced in January 2003 and became known as one of the most devastating Internet threats of the past decade. This worm continued to generate a great deal of traffic on the Internet in 2010.

Web content, spam, and phishing

- IBM Content security team identified that in the past three years, anonymous proxies have steadily increased, more than quintupling in number. Anonymous proxies are a critical type of website to track, because they allow people to hide potentially malicious intent.
- USA, India, Brazil, Vietnam, and Russia are the top five countries for spam origination in 2010.
- In 2010, spammers focused on content over volume. At the beginning of August, spammers began sending spam threats with ZIP attachments that contained a single EXE file that was malicious. By September, spammers began shifting to HTML spam to once again trick the end-user.
- There were a few months with ups and downs in the volume of spam seen over the year, however, the overall trends stayed flat and we have seen even less volume at the end of the year in comparison to the beginning of 2010.
- At 15.5 percent, India was the top country for phishing email origination in 2010, followed by Russia at 10.4 percent.
- In 2010, financial institutions continue to climb as the number one target for phishing attempts, representing 50 percent of the targeted industries up from the mid-year report when it was 49 percent.
- In 2010, more than three out of four financial phishing emails targeted banks located in North America. The remaining 22 percent targeted Europe.

Operating Secure Infrastructure

Vulnerabilities and Exploitation

- According to the X-Force database tracking, 2010 had the largest number of vulnerability disclosures in history—**8,562**. This is a 27 percent increase over 2009, and this increase has had a significant operational impact for anyone managing large IT infrastructures. More vulnerability disclosures can mean more time patching and remediating vulnerable systems.

- 49 percent of the vulnerabilities disclosed in 2010 were web application vulnerabilities. The majority of these were cross site scripting and SQL injection issues. However, as IBM X-Force has been saying for years, these vulnerabilities represent just the tip of the iceberg since many organizations develop third-party applications in-house that are never even reported publically and are not included in this count.
- Although vendors have been diligent in providing patches, at least 44 percent of all vulnerabilities in 2010 still had no corresponding patch by the end of the year.
- In early 2010, the term Advanced Persistent Threat (APT) became part of the everyday information security lexicon as a result of certain public disclosures and acknowledgement of a targeted series of attacks known as Operation Aurora. There has been much debate over this term and the underlying concepts within the information security community.
- During certain public disclosures in early 2010, and after attacks associated with Operation Aurora, the term APT began to take on a different meaning. In essence, APT became associated with any targeted, sophisticated, or complex attack regardless of the attacker, motive, origin, or method of operation.

Virtualization

- IBM X-Force notes that virtualization systems added 373 new vulnerabilities to the network infrastructure in the period between 1999 and 2009.
- A number of public exploits exist that demonstrate the risk from virtualization system vulnerabilities is real.
- Hypervisor escape vulnerabilities are the most common type of vulnerability that has been disclosed in server class virtualization systems.

Developing Secure Software

Web Application Vulnerabilities

- From the IBM® Rational® AppScan® OnDemand Premium Service we observed web application vulnerabilities comprising 49 percent of the total vulnerabilities reported in 2010, it is no surprise that developing secure software is harder than ever.
- In 2010 for the first time we now find that Cross-Site Request Forgery (CSRF) is more likely to be found in our testing than Cross-Site Scripting (XSS). This change is attributed to better detection techniques for CSRF and also a greater awareness of the risk. We find that organizations will tolerate having some outstanding issues with CSRF if the risk of exploitation is minimized. This is not the case with XSS and these issues are often quickly resolved.
- ASP.NET applications were clearly more susceptible to SQL injection than Java or PHP. The likely reason is that applications would typically use SQL Server as a backend database. SQL injection is better documented and easier to detect in this technology.
- As Web 2.0, AJAX applications, and Rich Internet Applications (RIAs) become more common, client-side JavaScript vulnerabilities may become more relevant, with a potential rise in the amount of such issues being exploited by malicious attackers.
- A recent IBM research study discovered that about 14 percent of the Fortune 500 sites suffer from many severe client-side JavaScript issues, which could allow malicious attackers to perform attacks such as
  - Infecting users of these sites with malware and viruses.
  - Hijacking users' web sessions and performing actions on their behalf.
  - Performing phishing attacks on users of these sites.
  - Spoofing web contents.
- Based on the dataset that we analyzed, we may extrapolate that the likelihood that a random page on the Internet contains a client-side JavaScript vulnerability is approximately one in 55.

Emerging Trends in Security

Mobile

- Mobile devices represent opportunities for sophisticated, targeted attackers. There are a number of vulnerabilities to target, and there is exploit information available.
- However, it is important to keep the vulnerability increases in perspective -- these do represent shared software components used by both mobile and desktop software. The vulnerability research that is driving these disclosures is not necessarily mobile-centric.
- Still, we aren't seeing widespread attack activity targeting mobile vulnerabilities today, because mobile devices do not represent the same kind of financial opportunity that desktop machines do for the sort of individuals who appear to create large Internet botnets.

Cloud security

- While security is still considered one of the major inhibitors to cloud adoption, organizations are increasingly adopting cloud-based technologies to address competitive market needs.
- Extending existing security policies and standards, leveraging sound physical security protections already in place, and assessing systems and applications for security weaknesses are examples of security design elements that should be included when establishing a secure cloud environment.

IBM Security collaboration

IBM Security represents several brands that provide a broad spectrum of security competency.

- IBM X-Force® research and development teams discover, analyze, monitor, and record a broad range of computer security threats and vulnerabilities
- IBM Managed Security Services (MSS) is responsible for monitoring exploits related to endpoints, servers (including web servers), and general network infrastructure. MSS tracks exploits delivered over the web as well as other vectors such as email and instant messaging.
- Professional Security Services (PSS) delivers comprehensive, enterprise-wide security assessment, design, and deployment services to help build effective information security solutions.
- Our Content security team independently scours and categorizes the web through crawling, independent discoveries, and through the feeds provided by MSS. In addition, the team actively monitors millions of email addresses to receive mass amounts of spam and phishing emails. This work provides optimal spam protection accompanied by the latest trends in spam and phishing emails.
- IBM has collated real-world vulnerability data from security tests conducted over the past three years from the IBM® Rational® AppScan® OnDemand Premium Service. This service combines application security assessment results obtained from IBM Rational AppScan with manual security testing and verification.
- IBM Cloud Security Services allows clients to consume security software features through a hosted subscription model that helps reduce costs, improve service delivery, and improve security.
- Identity and access management solutions provide identity management, access management, and user compliance auditing. These solutions centralize and automate the management of users, authentication, access, audit policy, and the provisioning of user services.
- IBM Endpoint Management Solutions combine endpoint and security management into a single offering that enables customers to see and manage physical and virtual endpoints—servers, desktops, roaming laptops, and specialized equipment such as point-of-sale devices, ATMs and self-service kiosks.

IBM Managed Security Services—A global threat landscape

IBM Managed Security Services (MSS) monitors several billion events in more than 130 countries, 24 hours a day, 365 days a year. The global presence of IBM MSS provides a first-hand view of current threats. IBM analysts use this wealth of data to deliver a unique understanding of the cyber threat landscape. This section focuses on Trojan botnet activity, SQL injection, obfuscation, PDF exploitation, and cross-site scripting activity—threats that are discussed throughout this report. The trend of these threats is vital to determining what direction the threat is taking and to understanding the significance of the threat to our networks.

Trojan Bot networks

IBM MSS saw an upward trend in Trojan botnet activity during 2010. This growth is significant because despite increasing coordinated efforts to shut down botnet activity (as seen with the Mariposa[1] and Bredolab[2] botnets), this threat appears to be gaining momentum. While there have been some successful shutdowns there are many botnets that, due to their resilient and sophisticated Command and Control (CnC) topology, remain largely unaffected by these takedown attempts. Another reason attributing to this growth is the availability of bot exploit toolkits such as WARBOT. This allows less than tech-savvy individuals to take advantage of the lucrative business of selling sensitive information on the black market.

Trojan Bot networks also continued to evolve in 2010. One of them, Zeus (also known as Zbot and Kneber), continues to evolve through intrinsic and plugin advances. The Zeus/Zbot family of botnets

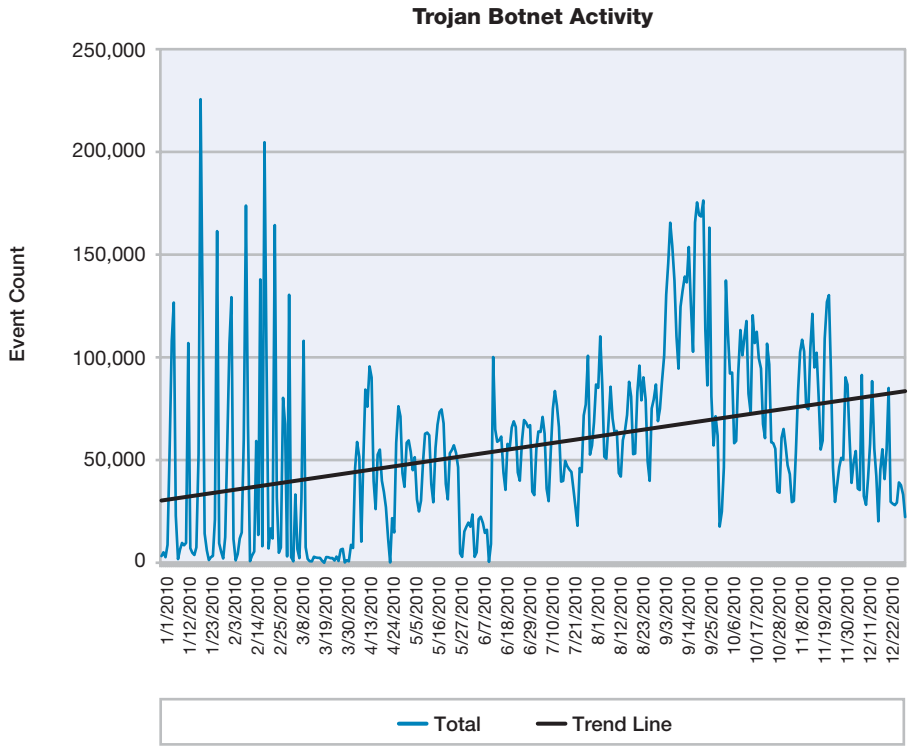

Figure 1: Trojan Botnet Activity

1 Massive Mariposa botnet shut down – http://www.net-security.org/secworld.php?id=8962
2 Bredolab botnet shut down – http://nakedsecurity.sophos.com/2010/10/26/bredolab-botnet-shut/

has been around for many years now and due to its extreme popularity with attackers, there are hundreds, or even thousands, of separate Zeus botnets active at any given time. The Zeus botnet malware is commonly used by attackers to steal banking information from infected computers.

Various bot networks based on Zeus are responsible for millions of dollars in losses over the last few years. For example, Zeus was reportedly responsible for stealing more than $1 million from customers of a single UK-based financial institution in July.[3] The continual arms race between attackers and defenders has botnet controllers finding stealthier ways to keep their bots under the radar. Zeus' merger with SpyEye, a very similar Trojan, is still in its infant stages. How this plays out over time is to be determined, but consolidation amongst Trojan botnets is expected to be an emerging trend.

In April, we saw a spike in malicious PDF activity associated with Zeus.[4] Attackers abused the "Launch" feature in Adobe Acrobat to distribute the Zeus botnet malware via email. The signature PDF_Launch_Program detects the network transfer of a PDF file containing an embedded action to Launch an executable program. Adobe Reader asks for user confirmation before actually launching the application, but certain versions of Foxit Reader do not and merely start the application without user confirmation. In cases where organizations have moved away from Adobe's implementation, this is of particular concern with regards to this attack.

Zeus' encrypted command and control activity is hard to detect. However, one of the signatures analyzed to assess this threat focuses on a type of behavior that Zeus might exhibit. The signature HTTP_Suspicious_Unknown_Content detects when a HTTP POST message results in a session where the content sent and received is not recognized as typical content, such as images or documents. Activity associated with this signature seemed to grow in intensity towards the latter half of 2010. Such activity could be normal or could indicate botnet activity. While this is a generic signature, we do believe that this activity is associated with Zeus. The section titled "Zeus botnet—facts, myths and understanding how these botnets operate" in the **2010 Mid-Year Trend and Risk Report** provides an in-depth explanation of Zeus and how readers can protect themselves from this threat.

There was also significant activity associated with the Waledac botnet at the start of the year up until early March and then the activity seemingly disappears for the rest of 2010. What could have caused this dramatic drop? We speculate that the cessation in activity is the result of "Operation b49".[5] This Microsoft led operation resulted in the takedown of a majority of this botnet in late February. Once a temporary restraining order was granted on February 22nd, much of the communication between Waledac's command and control centers and its thousands of zombie computers was cut off in a matter of days. In October, the U.S. District Court of Eastern Virginia ordered the permanent transfer of ownership of the 276 domains behind Waledac to Microsoft.[6] Does this mean that Waledac will never surface again? We may see activity, but probably not to the same magnitude that we observed prior to the takedown.

Another prevalent botnet is Pushdo (also known as Pandex and some components are known as Cutwail). This botnet generated noticeable activity across the IBM MSS network in 2010 though to a lesser extent than Waledac and Zeus. Pushdo, primarily used for spamming, had been observed launching Distributed Denial of Service (DDoS) attacks against certain SSL-enabled websites beginning in the first quarter 2010. The DDoS attack involved sending thousands of malformed SSL requests to the target hosts in an attempt to use up resources. To a business, this could directly impact revenue if services provided or product sales are interrupted during such an attack.

3 Targeted Attack Nets 3,000 Online Banking Customers – http://www.darkreading.com/smb-security/security/attacks/showArticle.jhtml?articleID=226600381
4 PDF-based Zeus attacks – http://www.iss.net/threats/PDFbasedZeusAttack.html
5 Cracking Down on Botnets – http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/02/24/cracking-down-on-botnets.aspx
6 R.I.P. Waledac – Undoing the damage of a botnet http://blogs.technet.com/b/microsoft_blog/archive/2010/09/08/r-i-p-waledac-undoing-the-damage-of-a-botnet.aspx

SQL injection

SQL injection is one of the leading attack vectors seen because of its simplicity to execute and its scalability to compromise large amounts of web servers across the Internet. A review of past X-Force Trend and Risk Reports reveals an interesting SQL injection trend. During each of the past three years, there has been a globally scaled SQL injection attack some time during the months of May through August. The anatomy of these attacks is generally the same: they target .ASP pages that are vulnerable to SQL injection. The surges that occurred during 2008 and 2009 are shown in Figure 2.

In 2008, attackers used a SQL CAST statement and some hex code to obfuscate the true injection string. The source of this attack was the Asprox botnet, and it was massively successful in compromising thousands of websites. In 2009, we observed the same attack methodology; the only difference was in the resulting payload. Asprox was again the source of this attack. However, it had varied success this time because of countermeasures that were deployed to thwart the attack.

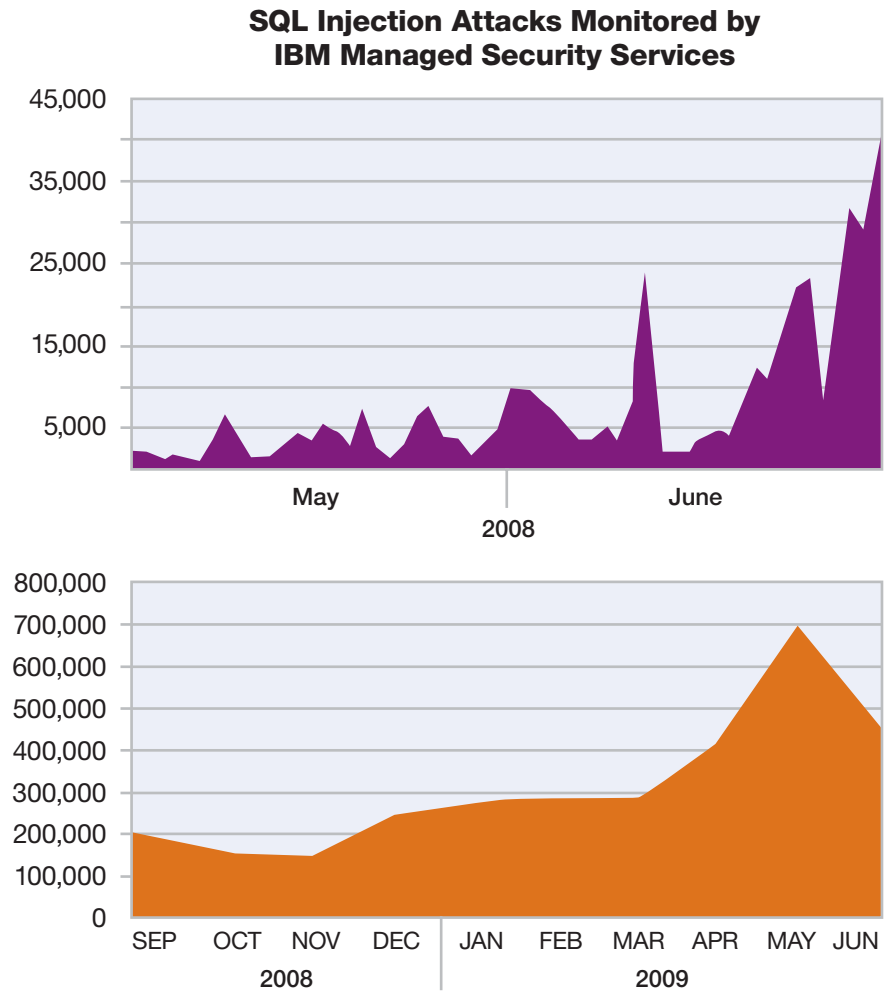

Figure 2: SQL Injection Attacks Monitored by IBM Managed Security Services

Figure 3 illustrates the significant SQL injection attack observed in 2010 as detected by the IBM signature SQL_Injection_Declare_Exec. The same attack methodology is used as in the previous two years, but some of the mechanics were changed. Attackers added leetspeak (1337) to the SQL statement to evade poorly written regex filtering. This statement, once decoded, contains another CAST statement resulting in two layers of obfuscation. While very similar to Asprox, this attack used slightly different techniques and therefore is known more popularly as the "dnf666" attack—so named because of a URL encoded inside.

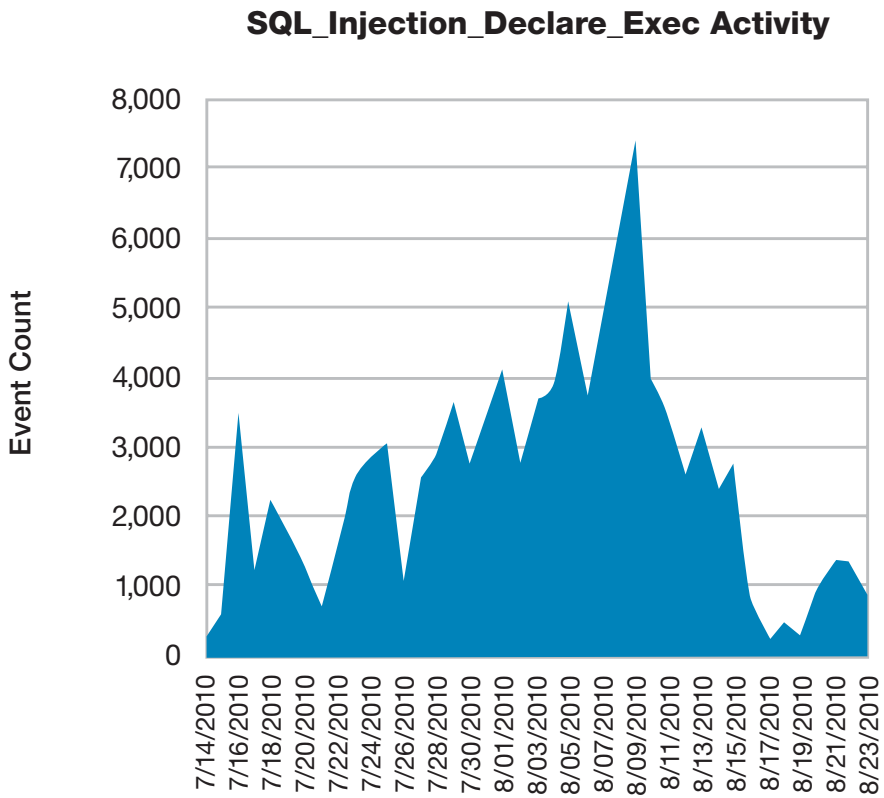

Figure 3: SQL_Injection_Declare_Exec Activity

Obfuscation

IBM MSS continues to track trends in obfuscation techniques used by attackers and toolkits. Obfuscation is a technique to hide or mask the code used to develop applications. New obfuscation methods are constantly evolving in an attempt to evade intrusion prevention systems (IPS) and anti-virus which often can't decode the web page or file to find the hidden attack. Through special detection algorithms incorporated into IBM Security Network IPS, we watch how patterns of use change by monitoring hits on these algorithms in our world-wide MSS deployments.

Obfuscation activity continued to increase during 2010 and shows no signs of waning. The most observed activity came from an event that triggers when a JavaScript 'unescape()' function with a large amount of escaped data is detected. This activity should be viewed with suspicion. It may be normal activity, or it could indicate the attempt to inject a large amount of shell code or malicious HTML and/or JavaScript for the purpose of taking control of a system through a browser vulnerability.

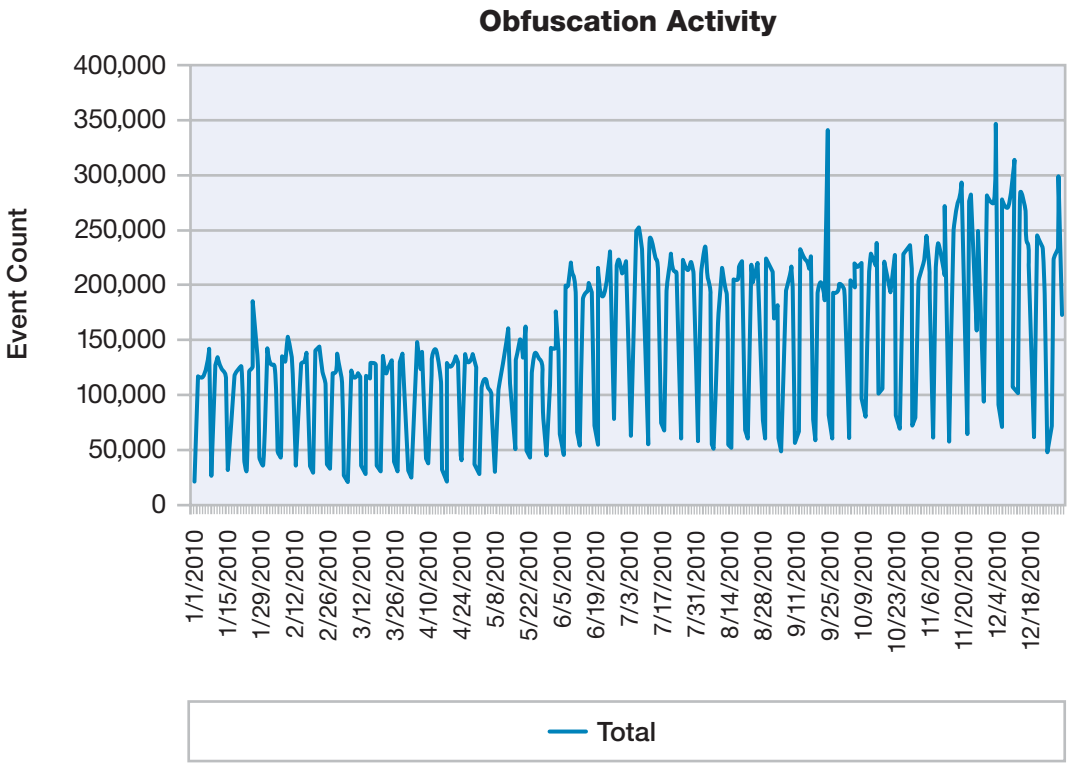

Figure 4: Obfuscation Activity

PDF exploitation

Compromise through PDF exploitation continues to be a favorite among attackers. Throughout 2010, our global Security Operation Centers witnessed surges of malicious traffic surrounding spam email. One notable increase occurred in late April, as shown in Figure 5. The emails of this particular spam campaign contained an Adobe Acrobat PDF that used the Launch command to deliver malware. At the peak of the attacks, IBM MSS received more than 85,000 alerts in a single day. The spam email was sent from various SMTP servers globally, which appeared to originate from the Zeus botnet.

There has been a small but steady rise in PDF exploitation since the beginning of 2010. There are numerous signatures that contribute to this assessment. Some of these signatures detect an unauthorized access attempt. For example, one signature detects a file with embedded corrupt JBIG2 data that could cause a buffer overflow in vulnerable versions of Adobe Acrobat and Adobe Reader. (Note: This is fixed in Adobe Acrobat/ Reader 8.1.3.) Other signatures may simply be looking for suspicious activity such as a PDF file containing a hex-encoded form of a filter name. This suggests malicious intent by concealing compressed content within the document.

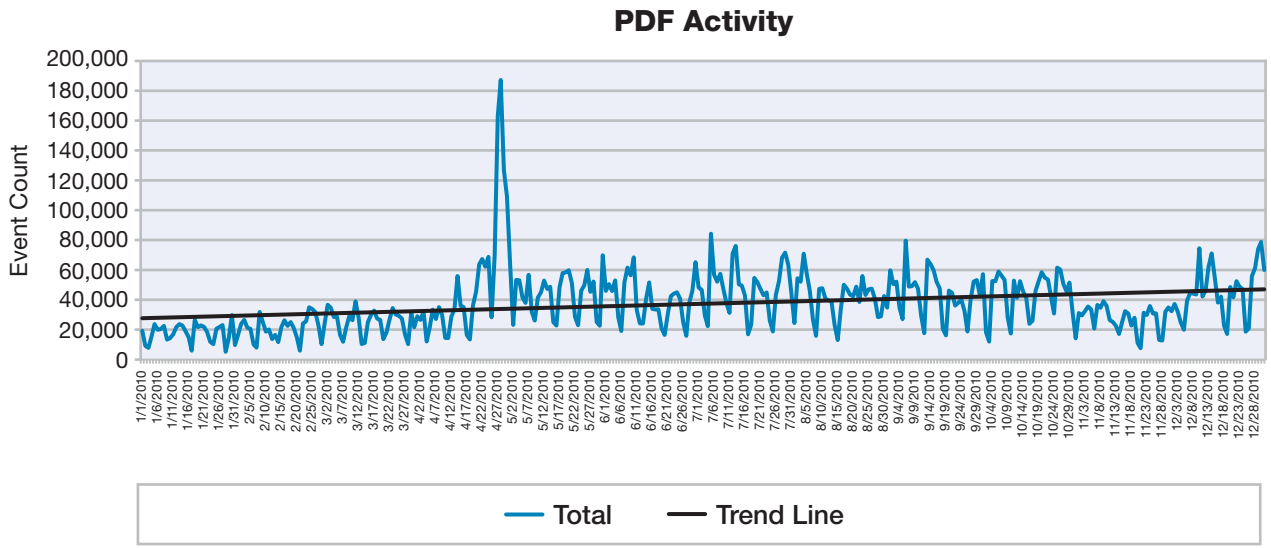

Figure 5: PDF Activity

Cross-site scripting

While cross-site scripting vulnerabilities continue to be one of the predominant types of vulnerabilities affecting web applications, activity targeting these vulnerabilities seems to have leveled off in 2010 as shown in Figure 6. Cross-site scripting allows attackers to embed their own script into a page the user is visiting, thereby manipulating the behavior or appearance of the page. These page changes can be used to steal sensitive information, manipulate the web application in a malicious way, or embed additional content on the page that can exploit other vulnerabilities.

Though the trend is flat, it does not mean that this threat is non-existent. From a Common Vulnerability Scoring System (CVSS) scoring perspective, these vulnerabilities do not typically rank as high or critical threats. IT and security professionals tend to deploy counter measures for the high-profile vulnerabilities first and, if resources allow, later address the low- to medium-rated issues. Attackers, therefore, will continue to take advantage of this window of opportunity in years to come.

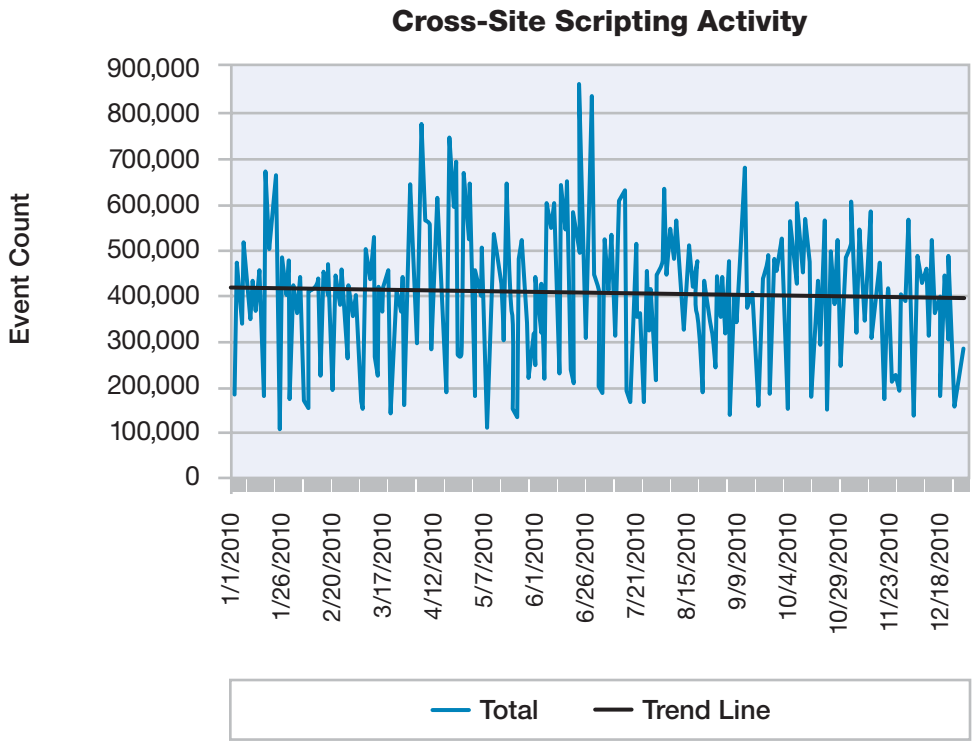

Figure 6: Cross-Site Scripting Activity

Industry trends

There is great interest in the general security community in knowing which industries are being targeted by what attack types. Our customer base is broad and reaches into a number of different industries. However, to identify a valid trend across a particular industry, we needed to establish a methodology with an acceptable sample size for analysis. For each attack category, we only assessed activity where a specific criterion was met in a given industry. A minimum number of affected customers and a minimum number of devices deployed amongst those customers was required prior to making an assessment.

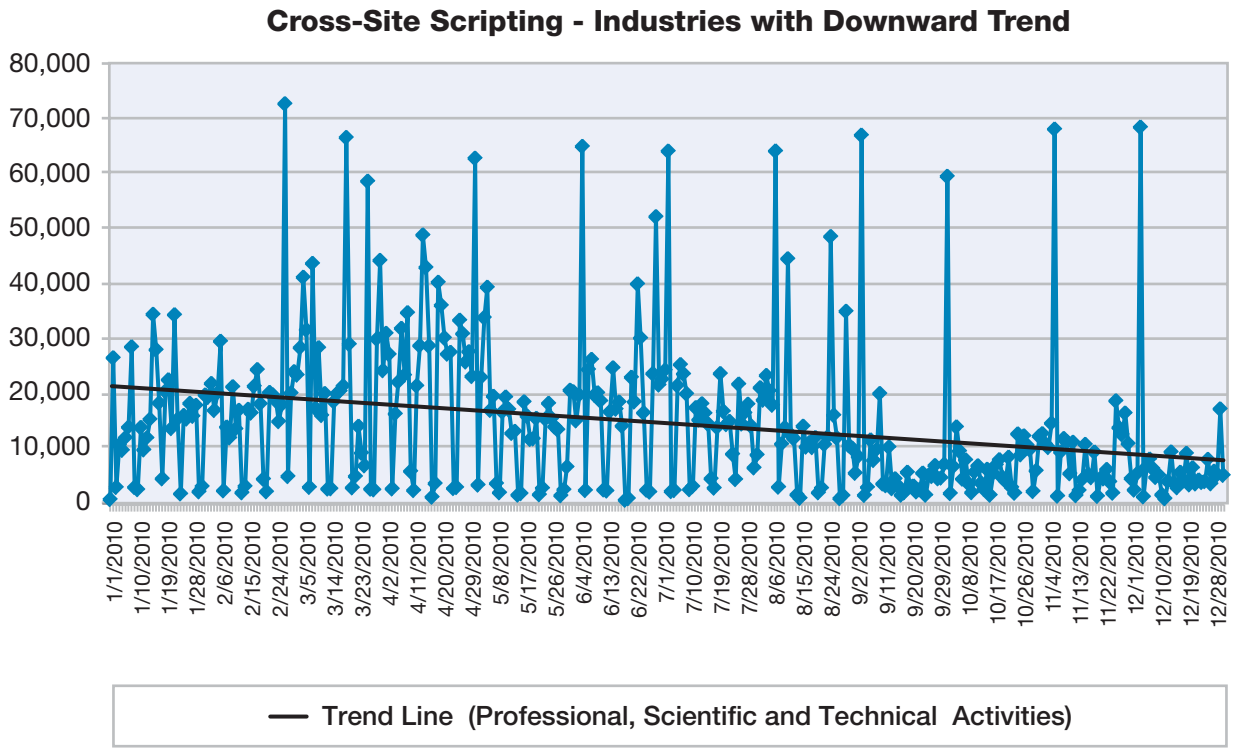

Figure 7: Cross-Site Scripting – Industries with Downward Trend

What did we see? Generally speaking, we did not see any significant discrepancies across different industries regarding the varying attack types compared to overall customer trends. Attack trends across all industries were relatively uniform.

What can be deduced from this? While some attacks are targeted, many exploits in circulation simply don't discriminate. A financial organization may be just as vulnerable to the latest botnet or PDF exploitation as an educational institution. Whether or not an organization is vulnerable to attack has much more to do with the protection measures that they have in place.

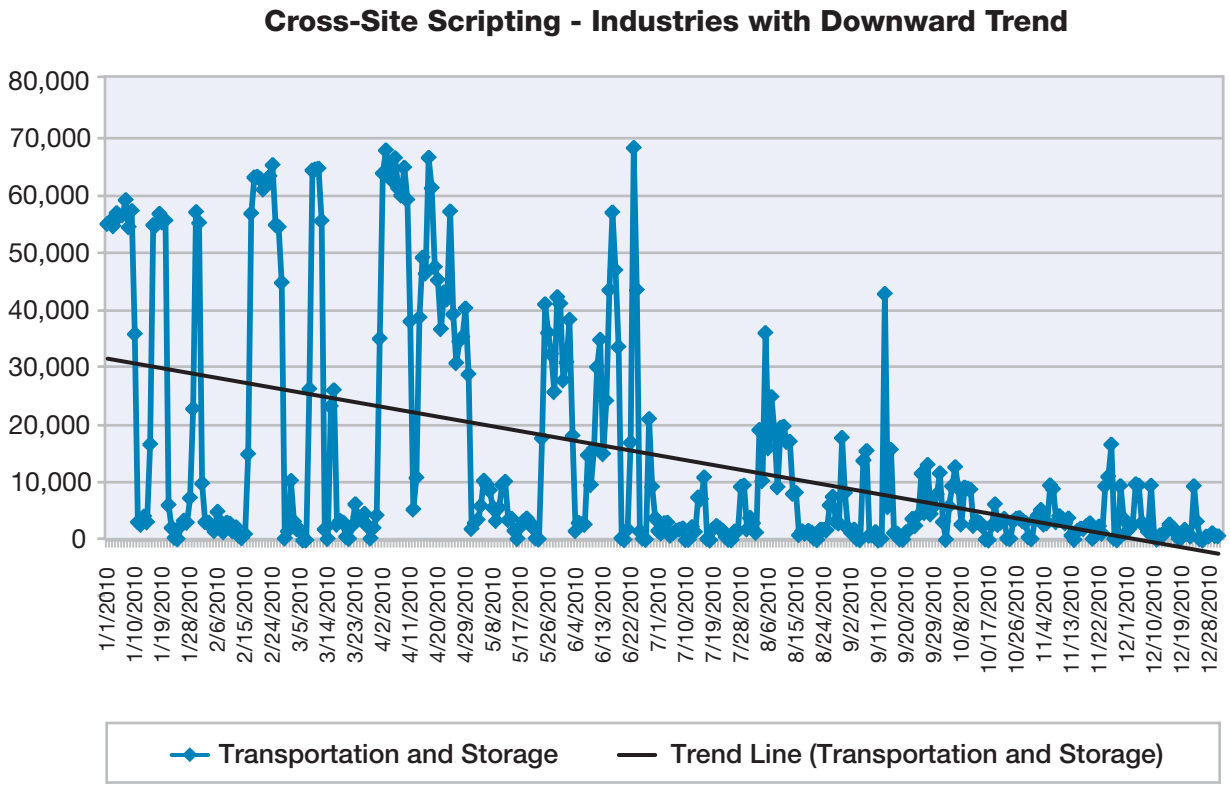

Figure 8: Cross-Site Scripting – Industries with Downward Trend

The only exception to our findings of consistent trends among the industries was in the cross-site scripting category. As shown in Figure 6, the overall trend for cross-site scripting was relatively flat and several industries followed this trend. As shown in Figures 7 through 9, a few industries saw a slight downward trend in this attack category including:

- "Professional and Scientific"
- "Wholesale and Retail Trade"
- "Transportation and Storage"

A decrease in cross-site scripting activity may indicate greater attention to addressing these types of vulnerabilities. **As noted later in this report, the IBM Rational AppScan on Demand Premium service that tracks web application vulnerabilities has also seen a steady decline in the instances of cross-site scripting reported vulnerabilities since 2007.** Part of this decline is attributed to a greater awareness of the risk associated with cross-site scripting.

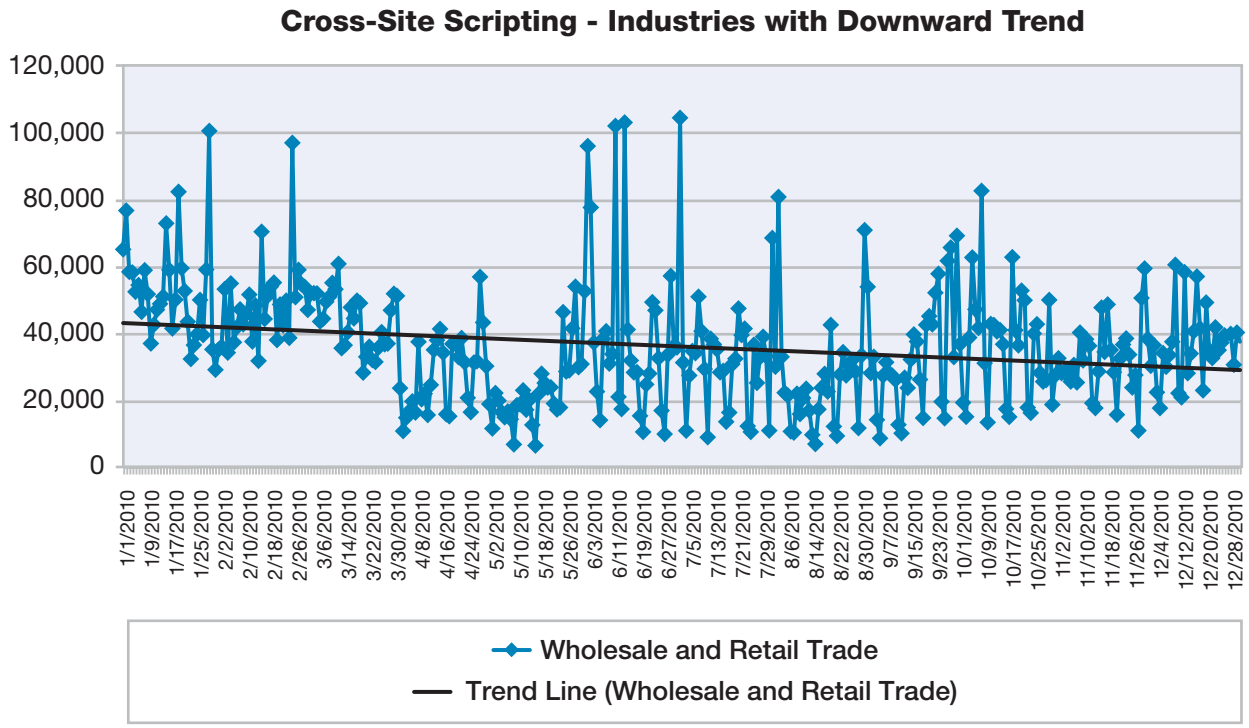

Figure 9: Cross-Site Scripting – Industries with Downward Trend

Top high-volume signatures—IBM MSS

Table 1 to the right, shows the placement of the top MSS high volume signatures and their trend line for 2010.

The top high volume signatures seen across the MSS network reveal some interesting aspects of life on the Internet today and are a reflection of the longevity of certain threats. For example, the SQL Slammer worm[7] first surfaced in January 2003 and became known as one of the most devastating Internet threats of the past decade. Despite the downward trend in 2010, this worm still exists and continues to propagate as evidenced by the top ranking signature, SQL_SSRP_Slammer_Worm shown in Table 1. SQL Slammer targets a buffer overflow vulnerability in the Resolution Service in Microsoft SQL Server 2000 or Microsoft Desktop Engine (MSDE) 2000 installations. This issue was patched by Microsoft in 2002. The fact that there is such a huge volume of activity associated with SQL Slammer seven years after it first surfaced probably suggests a need for better patch management.

Rank	Event Name	Trend Line
1	SQL_SSRP_Slammer_Worm	Down
2	SQL_injection	Down
3	PsExec_Service_Accessed	Slightly Up
4	SSH_Brute_Force	Slightly Down
5	JScript_CollectGarbage	Up
6	HTTP_Unix_Passwords	Slightly Up
7	SMB_Mass_Login	Down
8	SMB_Empty_Password	No Change
9	SQL_Empty_Password	Up

Table 1: Top MSS high volume signatures and trend line

7 SQL slammer traffic on the Internet significantly declined in March 2011 shortly before publication of this report. For more information on this topic, please see the Frequency-X blog. (http://blogs.iss.net/index.html)

Targeting SMB Servers

Two of the top signatures protect against threats targeting server message block (SMB) servers. The SMB_Empty_Password detects when a successful connection with no password is made to an SMB server. If this connection is from outside the network, consider the information on your server as compromised. The SMB_Mass_Login signature detects an excessive number of granted NetBIOS sessions originating from the same IP address. This may indicate a stolen account being used in a scripted attack. The existence of these signatures in the list highlights a possible lack of basic security with SMB shares. If attackers are attempting to connect to SMB servers with no password, this signifies that this method of attack continues to be fruitful for attackers. Recent threats, such as the Conficker and Stuxnet malware, use SMB shares to spread across networks.

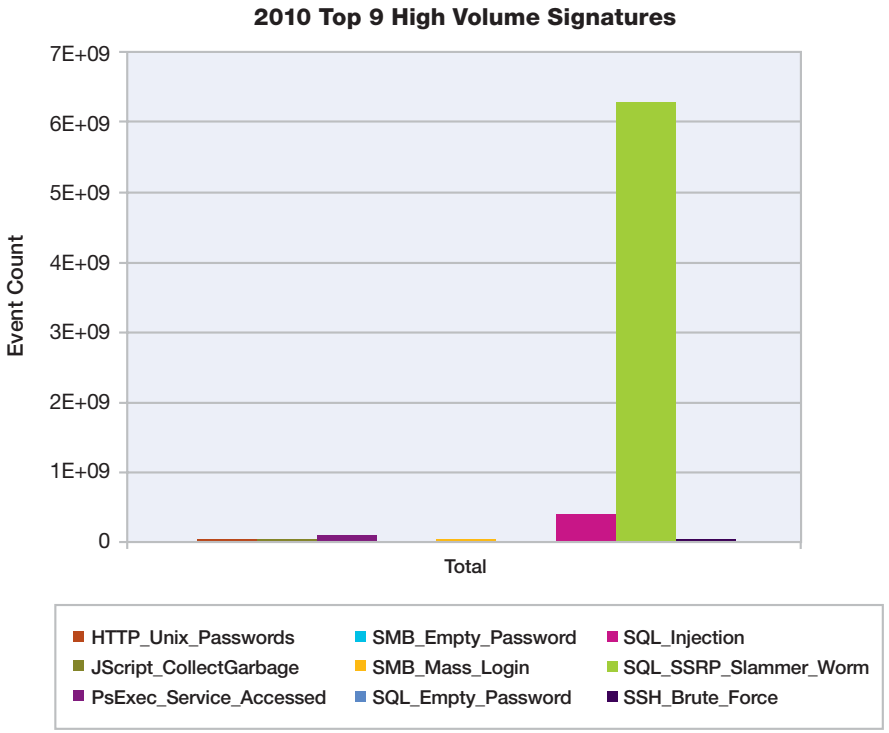

Figure 10a: 2010 Top 9 High Volume Signatures

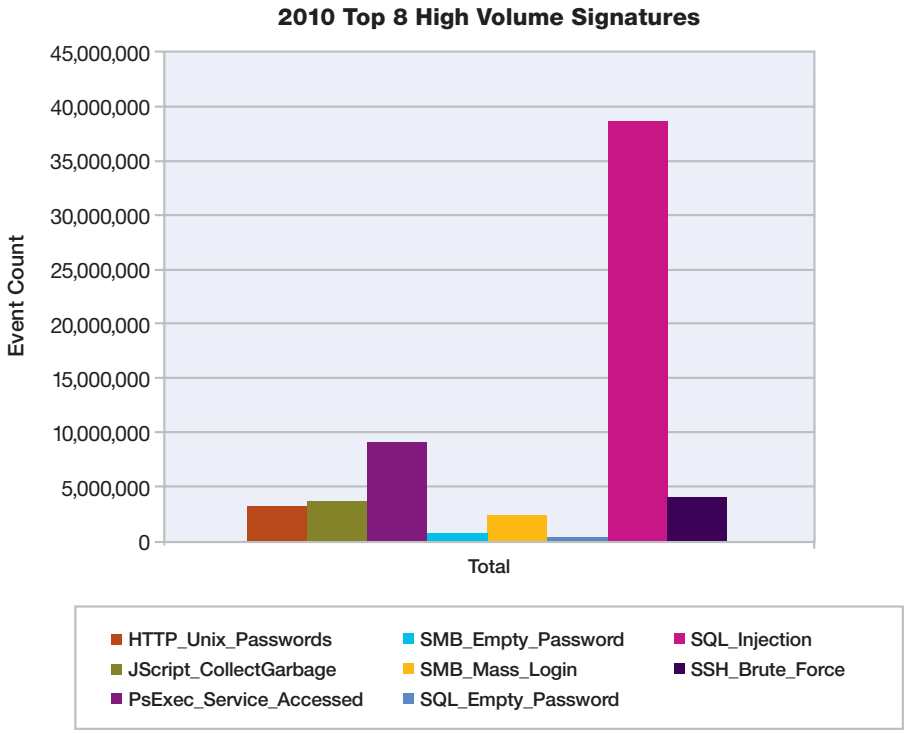

Figure 10b: 2010 Top 8 High Volume Signatures

SQL injection—high volume

Our heuristic SQL signature had the second highest volume seen in 2010. This is not surprising because SQL injection attacks against web applications are very common. IBM MSS has observed a seasonal surge in SQL injection attacks during the months of May through August for the past three years as discussed in the section **IBM Managed Security Services**—A global threat landscape. The other SQL signature noted in Table 1, SQL_Empty_Password, detects when a successful connection with no password is made to an SQL server. As with the SMB_Empty_Password signature, these types of connections should be considered suspicious if made from outside the network.

PsExec—A remote administration tool

The signature in the third spot, PsExec_Service_Accessed, is notable in that PsExec is a legitimate application. It is a command line based remote administration tool. However, worms and advanced threats also take advantage of PsExec. The "Here you have" worm, for instance, includes a PsExec tool that allows it to copy itself onto other computers over the network. If this application is used in your organization, you should ensure that best security practices are employed.

Brute force attacks & scans

SSH_Brute_Force is another interesting signature in this list. A brute force attack involves an attacker trying to gain unauthorized access to a system by trying a large number of password possibilities. This signature detects an excessive number of SSH Server Identifications from an SSH server within a specified timeframe. Through this type of attack, a malicious individual may be able to view, copy, or delete important files on the accessed server or execute malicious code. Organizations can help mitigate brute-force attacks by disabling direct access to root accounts and using strong usernames and passwords.

We provided an in-depth view on this topic in the **2010 Mid-Year Trend and Risk Report** where we explain the nature of a Darknet. A Darknet is a black-hole network whose addresses are not allocated to any active legitimate device or service on the Internet. When an attacker attempts a brute-force attack on a particular address in the Darknet they never connect to an SSH server because one does not exist. Therefore, they stop after one attempt. Conversely, a successful SSH connection may result in thousands of brute force attempts which explains the large volume of activity associated with SSH_Brute_Force.

The Darknet data in that mid-year report shows that the level of SSH brute force scanning is steadily increasing while the MSS data shows that the level of brute force attacks against active SSH servers is high.

JScript & UNIX

JScript_CollectGarbage detects the transfer of a JScript file containing a call to the function CollectGarbage(). CollectGarbage() is part of the .NET framework but, according to Microsoft, "is not intended to be used directly from your code." This function has been used by attackers and can be indicative of malicious intent. However, it can also be used for legitimate purposes.

Finally, the HTTP_Unix_Passwords signature detects attempts to access the /etc/passwd file on UNIX systems via a web (HTTP) server. While this activity is sometimes authorized, it can sometimes be suspicious. This is a very old attack, but is still successful today.

Trending in the dark—what does malicious traffic look like?

As we discussed in the previous section, one of the many data resources that IBM security analysts use to determine trending is the darknet, also known as a black-hole network. A darknet is a large range of IP addresses on the Internet that have never had any services running on them. Our darknet has an aperture of 25,600 addresses. Generally speaking, there is no legitimate reason why computers on the Internet would send packets to addresses in this range, but in fact they do. Often, traffic into this network is associated with malicious activity. This space is continuously monitored and all incoming traffic is captured in its entirety and stored for analysis and long-term archiving.

Spoofed Denial of Service attacks

Looking at the data over the past several years, a couple of patterns begin to emerge. The first trend is the gradual rise in backscatter activity (Figure 11). Backscatter is actually a side effect of a spoofed Denial of Service (DoS) attack. Attackers launching Denial of Service attacks on the Internet will often put incorrect source addresses in the packets they are flooding at their victim. This is known as spoofing. By spoofing randomly selected source addresses, the attacker makes it difficult for the victim's system to distinguish between the spoofed packets and legitimate packets from real users. The victim system will respond to a certain percentage of these spoofed packets. These responses are known as backscatter. If an attacker randomly selects an IP address in our darknet range, and the victim responds, we'll collect that response. By studying these responses we can learn things about Denial of Service activity on the Internet.

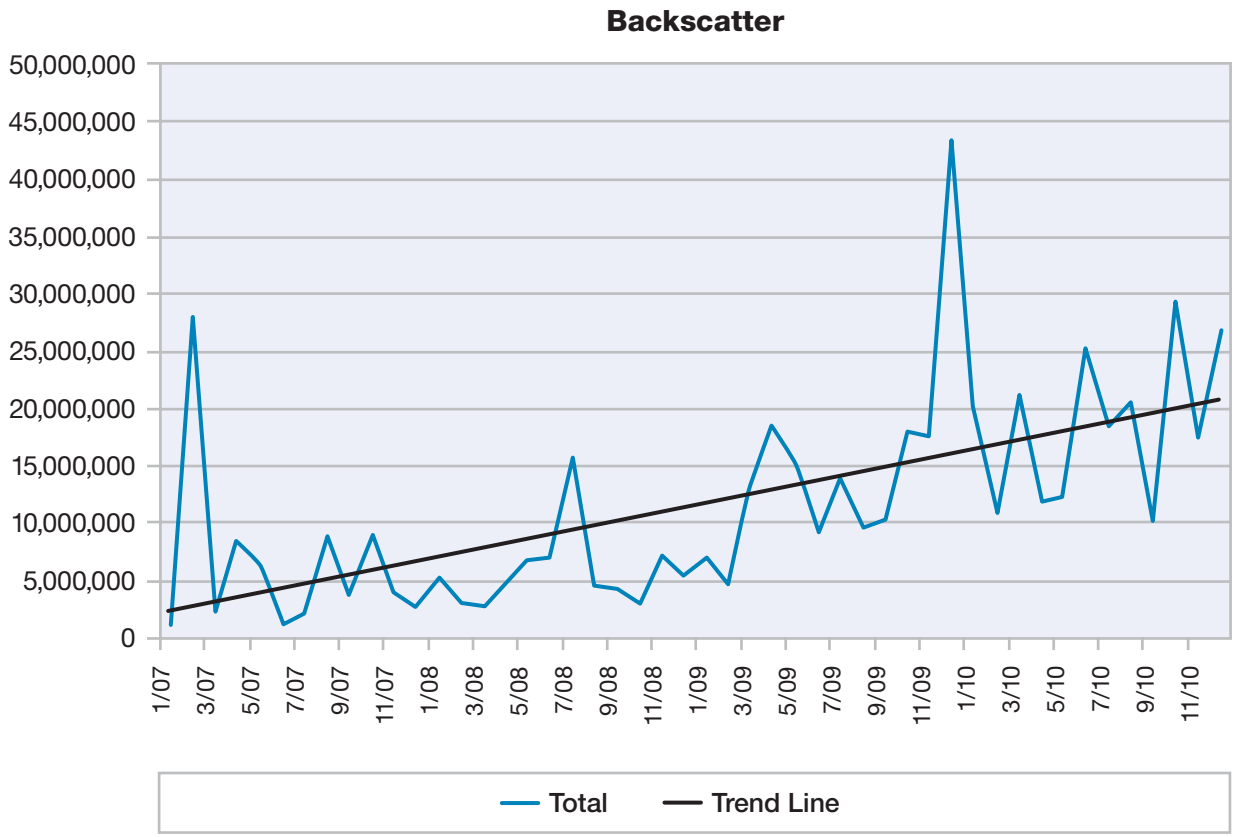

Figure 11: Backscatter

In the X-Force darknet, each SYN-ACK backscatter packet received is an indicator that an attacker sent a spoofed packet to a well-known service port on the machine under attack spoofed from one of X-Force darknet addresses. While there has been a gradual increase in backscatter activity since 2007, there was a large jump year-over-year between 2008 and 2009. Part of this increase is due to a significant spike in activity in 2009—the largest in the three and half year period. This trend of higher than previous year averages continues in 2010. At the close of Q2, the average count for the first half of 2010 is slightly higher than the total average for 2009, just over 16.5 million. At the close of the year 2010 we see that this number has now jumped to over 18 million. Figure 12 indicates the increase in volume from 2007 through 2010 of spoofed Denial of Service attacks on the Internet.

What can we deduce from this gradual rise in backscatter data and, in some instances, large jumps of backscatter activity? Since the majority of the backscatter data results from Denial of Service (DoS) attacks, we can speculate that there has been a steady increase in spoofed DoS attacks since 2007. However, backscatter is subject to a high degree of variability due to the nature of what is being collected and what is occurring. Some intense periods of backscatter are the result of internecine warfare within and between various attacker camps. During this warfare, one group attempts to block or take over the resources of another group. This "shelling match" between warring camps can result in a sudden increase in backscatter traffic and backscatter source addresses. It generally ceases as suddenly as it began. This type of activity most likely contributed to the dramatic spikes in February 2007 and December 2009 as shown in Figure 11 on page 24.

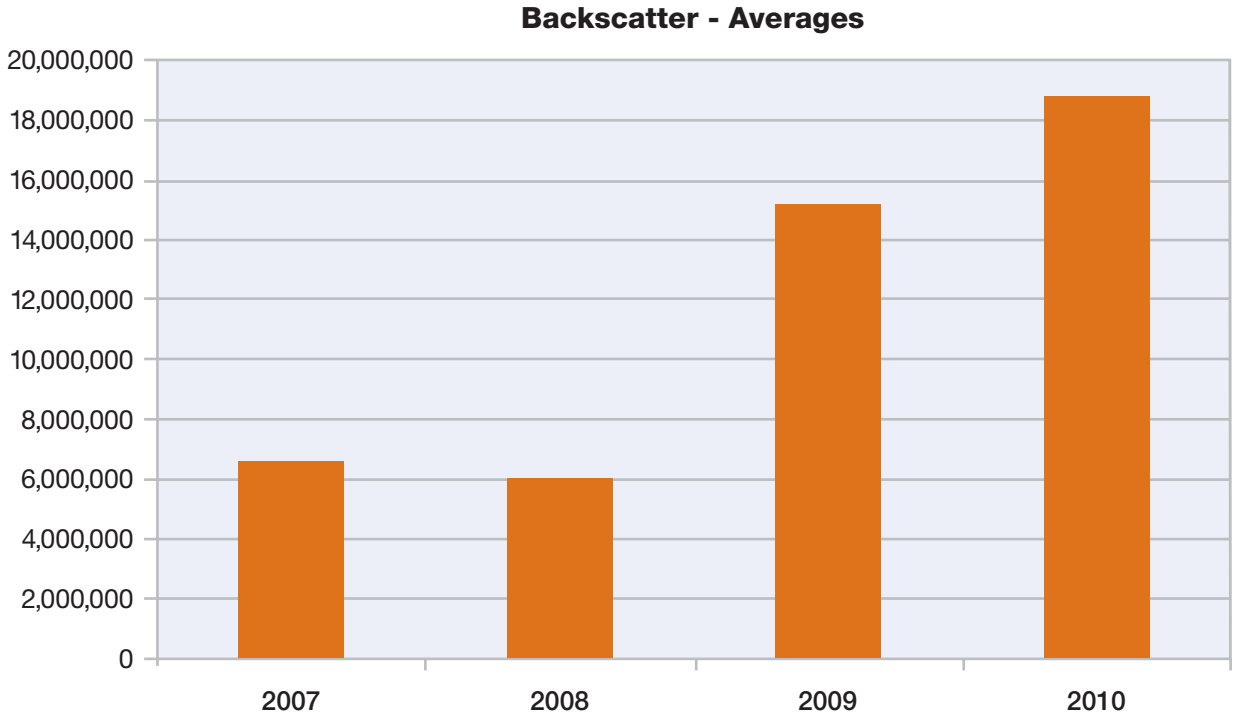

Figure 12: Backscatter – Averages

Targets of Denial of Service attacks

The nature of a spoofed Denial of Service attack makes it difficult to determine the attacker. The attacker fabricates origins for the connections to the victim's IP address. These fabricated connections can in turn come from a multitude of different machines. When looking at backscatter in the X-Force darknet, it is clear that the origins of the attack are spoofed, but the target of the attack is known. Examining the sources of the backscatter provides information on the targets of spoofed Denial of Service attacks. Figure 13 shows the top backscatter-generating countries for the second half of 2010 as calculated using the WorldIP database that maps addresses to countries.

There is a fairly common trend in the data. The United States is by far the largest generator, China is second, and Turkey is third. The United States and China have the first and second largest counts of IP addresses so their ranking as backscatter generators isn't surprising. If any IP address is as likely to be a target as any other then one would expect to see Japan, Germany, South Korea, or the UK in the top three. This assumption is clearly wrong. Further analysis and correlation with other data may help shed light on the matter.

For more discussion about brute force attacks and the information reported earlier in the year, please refer to the **2010 Mid-Year Trend & Risk report** located on our web page under report archives.

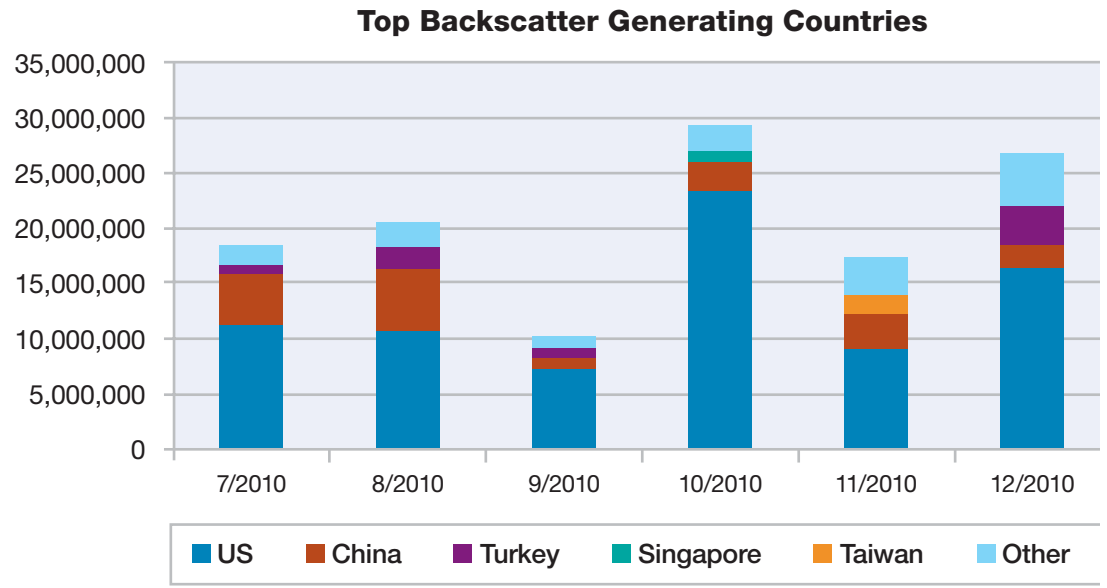

Figure 13: Top Backscatter Generating Countries

Worms of yesteryear: Where are they now?

The ongoing war against the threat of computer worms is cyclic. A new invader appears, after the battles to contain the infection and the initial outbreak appears won, it falls off the collective radar as years pass and the next invaders appear.

Worms propagate by a number of methods such as malicious email attachments, open or weakly protected shares and network accessible software vulnerabilities. A number of prominent worms have appeared over the last seven years but those that spread via exploitation of network accessible vulnerabilities tend to be the most virulent. They can spread across networks from machine to machine without a user interceding to view an email or open a file. The autonomous spreading of these worms can lead to high infection rates and frequently, disastrous side effects occur of machines crashing from unreliable exploitation and potentially crippling network utilization for virulent worms.

IBM's Managed Security Service tracks the malicious activity seen on its customer's networks and thus affords a window into the activity of these worms of yesteryear. The following list gives an overview of five of the most recent worms that spread entirely or partly by exploiting operating system vulnerabilities. All of these worms targeted software, usually operating systems, by Microsoft.

SQL Slammer first appeared in late January of 2003, generating such a deluge of traffic that it brought down numerous critical resources and noticeably slowed the Internet. Its single UDP packet payload targeted a vulnerability in Microsoft SQL Server that had been patched previously in July. The compromised host would then loop, spamming copies of itself to random IP addresses, DoSing (Denial of Service) itself and sending out a large amount of traffic.

Blaster appeared in August of 2003 and rapidly spread. This worm propagated by exploiting a buffer overflow in the Remote Procedure Call (RPC) interface and the Distributed Component Object Model (DCOM) interface that had been patched a month earlier. The worm payload would install an auto-starting executable that would continue trying to propagate and trigger a Denial of Service against Microsoft's update site at a specific time.

Sasser appeared at the end of August in 2004. It propagated by exploiting a vulnerability in the Local Security Authority Subsystem Service (LSASS), which is a process in Microsoft Windows operating systems that is responsible for enforcing the security policy on the system. LSASS patched a few weeks previously. Once infected, a machine would download and install an auto-starting executable which would scan and attempt to infect other machines. The worm itself wasn't malicious but a side effect of its scanning caused crashes and reboots in servers and desktops which had severe consequences for many companies.

The **Zotob** worm appeared in mid-August of 2005. It propagated by exploiting a buffer overflow in the Microsoft Plug and Play service that was patched earlier in the month. A side effect of this propagation was crashing and reboots of machines due to the exploit. Infected machines would download and install an executable to continue propagation and install a backdoor to phone back to an Internet Relay Chat (IRC) channel for further instructions.

Conficker was detected in early November of 2008. Propagation was via a vulnerability in the server service of all supported Microsft operating systems at the time. Later variants added additional vectors such as weak SMB passwords and infection of USB devices. Once compromised, the infected machine would attach itself to a botnet awaiting further commands. Most variants of this worm also performed controlled scanning and infection of further hosts.

Year	Worm	Vulnerability	IBM Signature	MS Bulletin
2003	SQL Slammer	CVE-2002-0649	SQL_SSRP_StackBo	MS02-039
2003	Blaster	CVE-2003-0352	MSRPC_RemoteActivate_Bo	MS03-026
2004	Sasser	CVE-2003-0533	MSRPC_LSASS_Bo	MS04-011
2005	Zotob	CVE-2005-1983	PlugAndPlay_BO	MS05-039
2008	Conficker	CVE-2008-4250	MSRPC_Srvsvc_Path_Bo	MS08-067

Table 2: Top Worms 2003 - 2008

Figure 14 breaks down the alert activity by worm. For clarity, the alert associated with the worm activity has been renamed for the worm. In most cases this network activity is based on detected exploitation by the worms but this is a tricky endeavor for a number of reasons. For one, the alert is not necessarily an indication of an attempted propagation by a worm, alerts can be due to a security audit or an exploitation attempt by something else entirely. Another issue is that worms have different propagation rates. Conficker regulates its propagation in an attempt to avoid overt detection while SQL Slammer can spam hundreds of exploitation attempts a second. Due to the number of ways that Conficker variants can spread, counts of peer to peer activity were used.

SQL Slammer[8] has by far the largest number of exploitation attempts. Even though seven years have passed in which time to remediate the worm, it remains extremely noisy. The large dip in activity between July and August is due to remediation in a single network. Ever afterwards, Slammer counts overshadow all others.

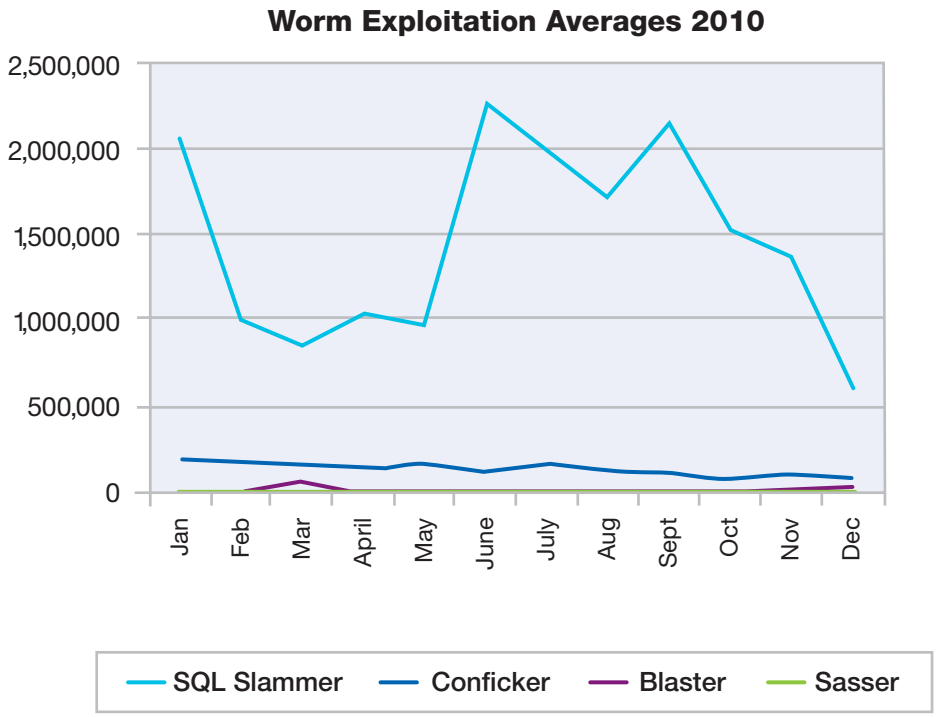

Figure 14: Worm Exploitation Averages 2010

8 SQL slammer traffic on the Internet significantly declined in March 2011 shortly before publication of this report. For more information on this topic, please see the Frequency-X blog. (http://blogs.iss.net/index.html)

Figure 15 shows the same monthly averages with SQL Slammer removed. Conficker traffic is the next highest. This is not surprising as it is the most recent of the studied worms and also known to be extremely widespread. There is a noticeable decline in activity over the year, likely attributed to infected nodes being cleaned or brought offline. Blaster and Sasser are still showing activity while Zotob's counts were so low that it was removed from the figure. This discrepancy may be due to the fact that Blaster and Sasser would affect both Windows 2000 and XP and they came at an earlier time while Zotob only affected Windows 2000 and came out in 2005.

It is interesting to note, that the worms exploiting vulnerabilities patched over seven years ago still show noticeable activity. The activity for all the worms is unlikely to grow significantly as any new machine brought online should not be vulnerable to the exploits they spread by. It seems inevitable that the activity from these worms will eventually die out as old infected machines are replaced but they do show a remarkable tenacity.

New worms will always be on the horizon. As the latest invader is brought under control and gradually driven out, it will likely never be fully ousted. There will almost certainly be a few survivors holding out in the dark corners of our networks.

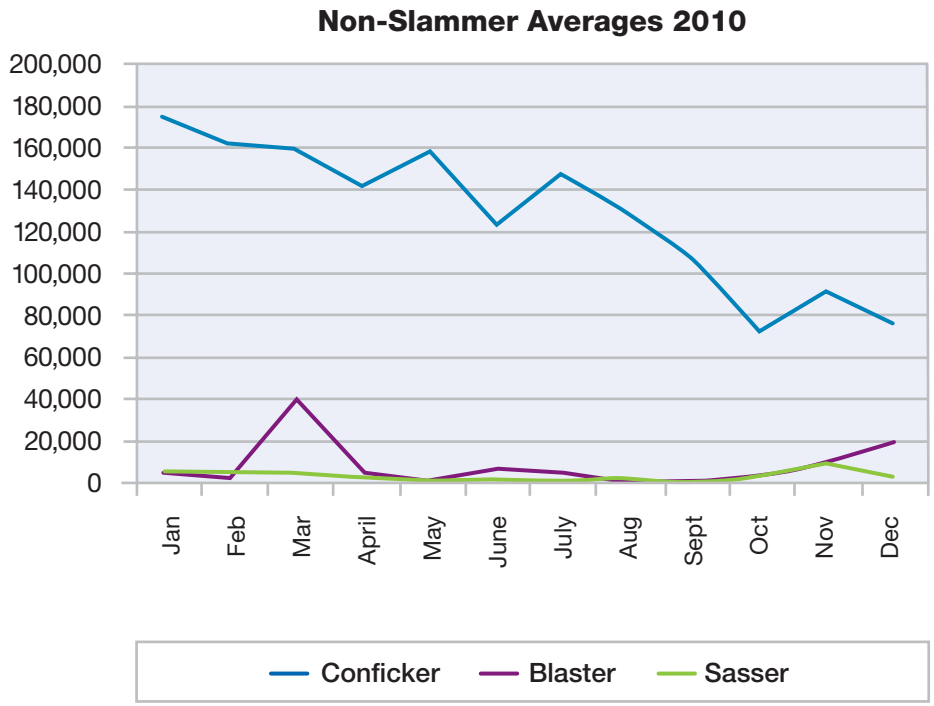

Figure 15: Non-Slammer Averages 2010

Web content trends

This section summarizes the amount and distribution of "bad" web content that is typically unwanted by businesses based on social principles and corporate policy. Unwanted or "bad" Internet content is associated with three types of websites: adult, social deviance, and criminal.

The web filter categories are defined in detail at: **http://www-935.ibm.com/services/us/index.wss/detail/iss/a1029077?cntxt=a1027244**

Table 3 below lists the IBM web filter categories that correspond with these types of sites.

This section provides analysis for:

- Percent and distribution of web content that is considered bad, unwanted, or undesirable
- Increase in the amount of anonymous proxies
- Malware URLs: Hosting countries and linkage

Website Type	Description & Web Filter Category
Adult	Pornography Erotic / Sex
Social Deviance	Political Extreme / Hate / Discrimination Sects
Criminal	Anonymous Proxies Computer Crime / Hacking Illegal Activities Illegal Drugs Malware Violence / Extreme Warez / Software Piracy

Table 3: Web filter categories associated with unwanted web content

Analysis methodology

X-Force captures information about the distribution of content on the Internet by counting the hosts categorized in the IBM Security Solutions web filter database. Counting hosts is a method for determining content distribution and generally provides a realistic assessment. Results may differ when using other methodologies such as counting web pages and sub-pages.

The IBM Content data center constantly reviews and analyzes new web content data. The IBM Content data center analyzes 150 million new web pages and images each month and has analyzed 14 billion web pages and images since 1999!

The IBM Web Filter Database has 68 filter categories and 67 million entries with 150,000 new or updated entries added each day.

Percentage of unwanted Internet content

Approximately seven percent of the Internet currently contains unwanted content such as pornographic or criminal websites.

Increase of anonymous proxies

As the Internet becomes a more integrated part of our lives—not only at home, but at work and at school—organizations responsible for maintaining acceptable environments increasingly find the need to control where people can browse in these public settings.

One such control is a content filtering system that prevents access to unacceptable or inappropriate websites. Some individuals attempt to use an anonymous proxy (also known as web proxies) to circumvent web filtering technologies.

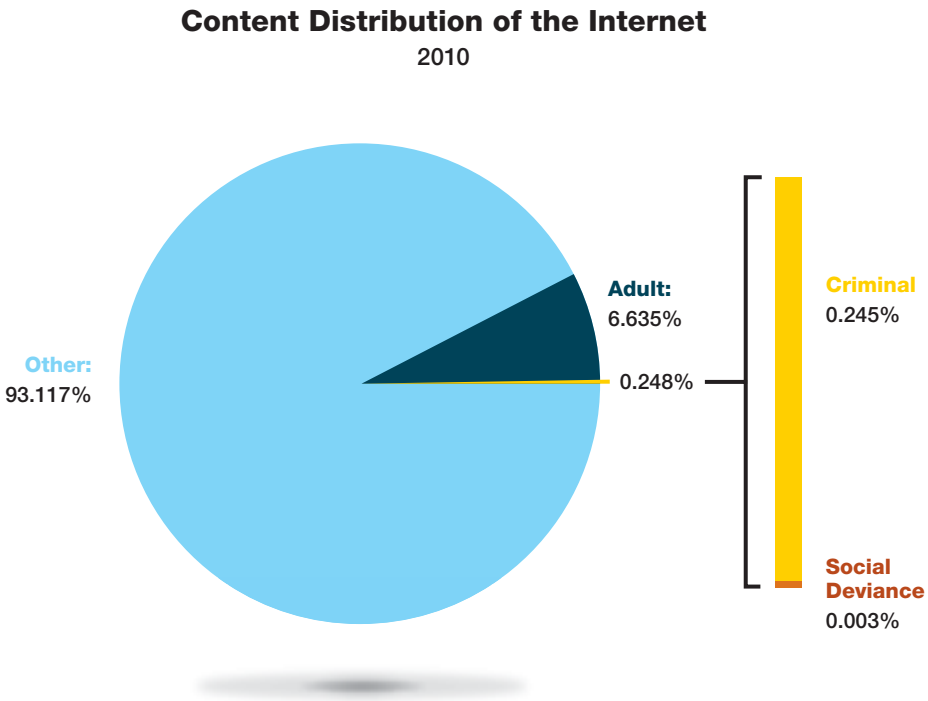

Figure 16: Content Distribution of the Internet – 2010

Web proxies allow users to enter a URL on a web form instead of directly visiting the target website. Using the proxy hides the target URL from a web filter. If the web filter is not set up to monitor or block anonymous proxies, then this activity (which would have normally been stopped) can bypass the filter and allow the user to reach the disallowed website.

The growth in volume of anonymous proxy websites reflects this trend.

In the past three years, anonymous proxies have steadily increased, more than quintupling in number. Anonymous proxies are a critical type of website to track, because of the ease at which proxies allow people to hide potentially malicious intent.

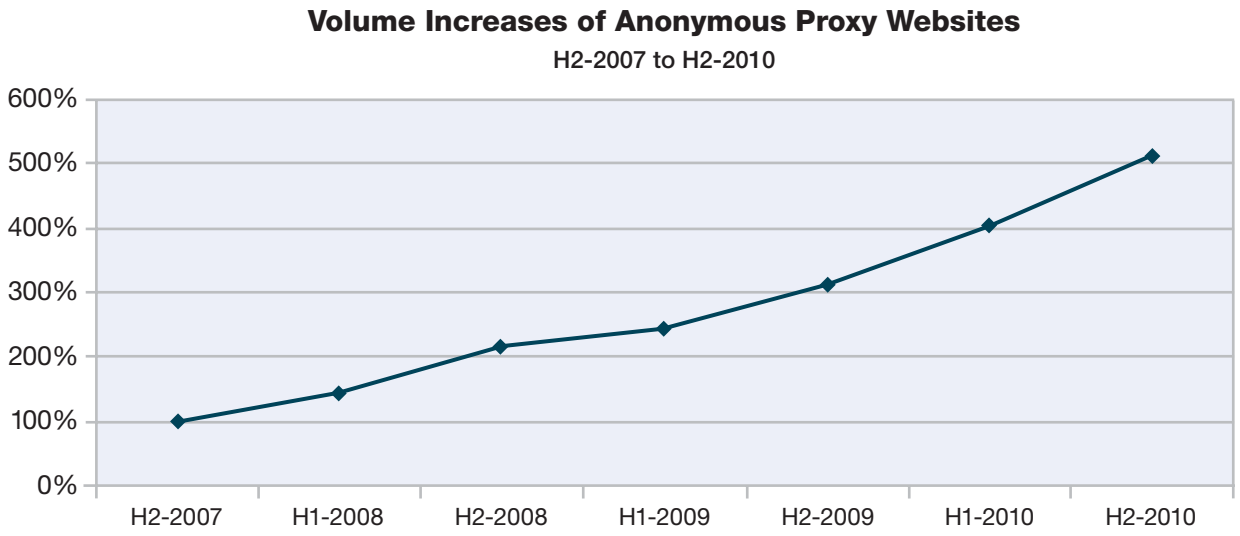

Figure 17: Volume Increases of Anonymous Proxy Websites – H2-2007 to H2-2010

Top Level Domains of Anonymous Proxies

Figure 18 illustrates the Top Level Domains (TLDs) of the newly-registered anonymous proxies.

In 2006, more than 60 percent of all newly-registered anonymous proxies were .com domains, but since the middle of 2007, .info has been at the top until the beginning of 2010 (while .com was runner-up most of the time).

But why is .info no longer in the prime position? It seemed to be a proven TLD for anonymous proxies for years. A reason could be that .info, similar to .com, is running out of names. Additionally, the question arises why anonymous proxies are now provided on .cc and .tk top level domains. These are the Domains of Cocos (Keeling) Islands (.cc), an Australian territory, and Tokelau (.tk), a territory of New Zealand. Nearly all .cc anonymous proxy websites are registered on the domain co.cc. It is free of charge to register a domain anything.co.cc (see **http://www.co.cc/?lang=en**). The same is true for .tk. (see **http://www.dot.tk/**). Thus, it is both cheap and attractive to install new anonymous proxies on .co.cc or .tk.

Additional trends:

- At the end of 2009, .cc (Cocos (Keeling) Islands) started to increase significantly and even reached the number one position in the second quarter of 2010. Nevertheless .cc went out of vogue by the end of 2010.

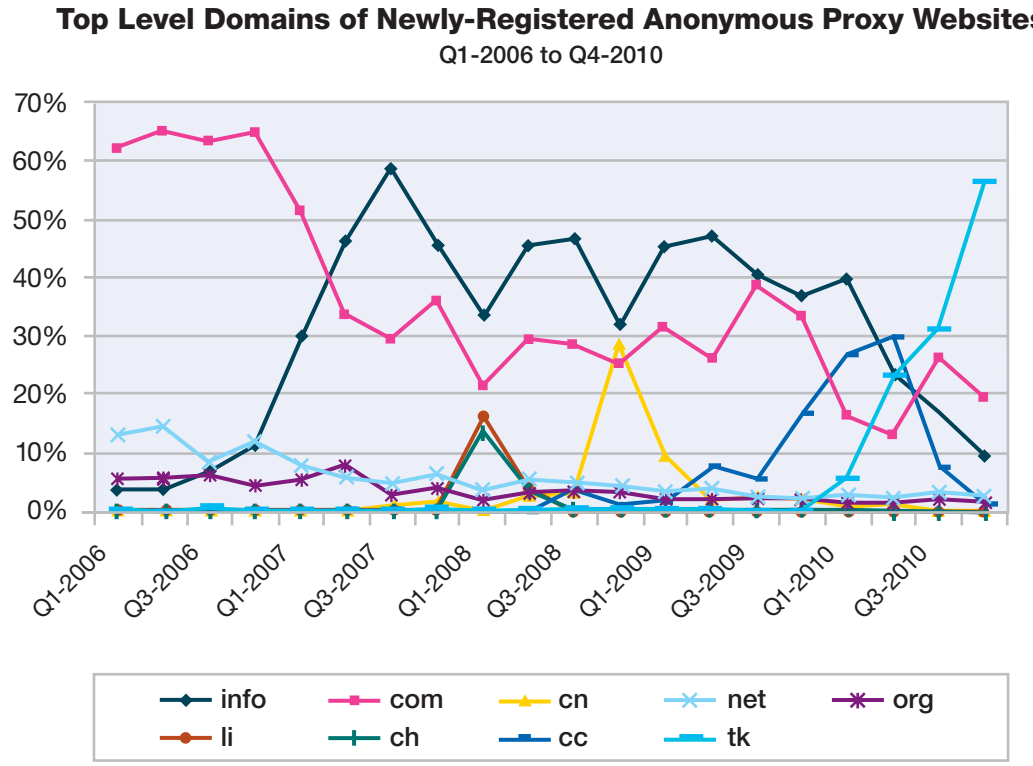

Figure 18: Top Level Domains of Newly-Registered Anonymous Proxy Websites – Q1-2006 to Q4-2010

- In the second quarter of 2010, another new star in proxy heaven, .tk (Tokelau), reached about 23 percent of new anonymous proxies. It dominated the rest of the year by acquiring nearly 30 percent in the third quarter and more than 56 percent in the fourth quarter of 2010.
- During that same time period, .info decreased dramatically and fell below 10 percent for the first time by the end of 2010.
- In the first quarter of 2010, even .com fell significantly below 20 percent for the first time, recovering to 26 percent and then 19 percent in the third and the fourth quarters of 2010.

It will be interesting to see whether .tk has a similar destiny as .co.cc—being the star of anonymous proxies for a year and a half before declining.

Country hosts of anonymous proxy websites

For anonymous proxy hosting countries, the United States has held the top position for years. More than 70 percent of all newly registered anonymous proxies were hosted in the U.S. for the years 2006-2009. In the third quarter of 2010 they fell below 70 percent for the first time in more than four years, but recovered to nearly 72 percent by the end of 2010.

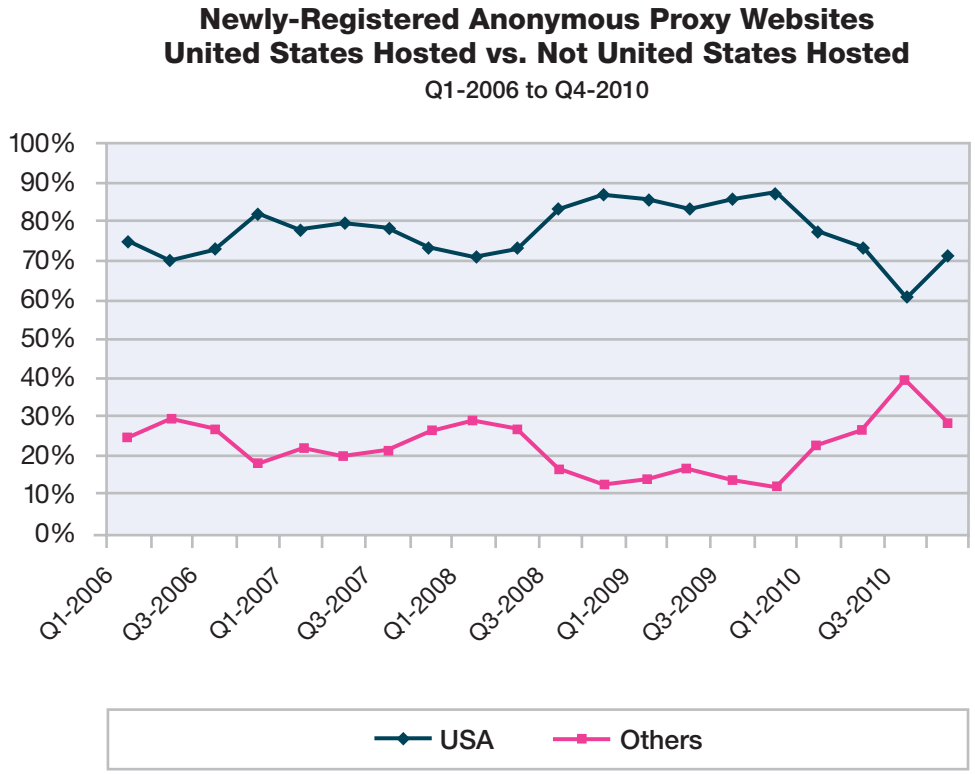

Figure 19: Newly-Registered Anonymous Proxy Websites United States Hosted vs. Not United States Hosted – Q1-2006 to Q4-2010

It is worth looking at the remaining 30 percent of all newly registered anonymous proxies in 2010. This remainder is dominated by UK (9 percent in the third quarter of 2010), Canada (6.4 percent in the third quarter of 2010), and Netherlands (5.8 percent in the third quarter of 2010). Thus, those three countries made up more than 20 percent in the third quarter of 2010. All other countries host less than 4.5 percent at the time of press in 2010.

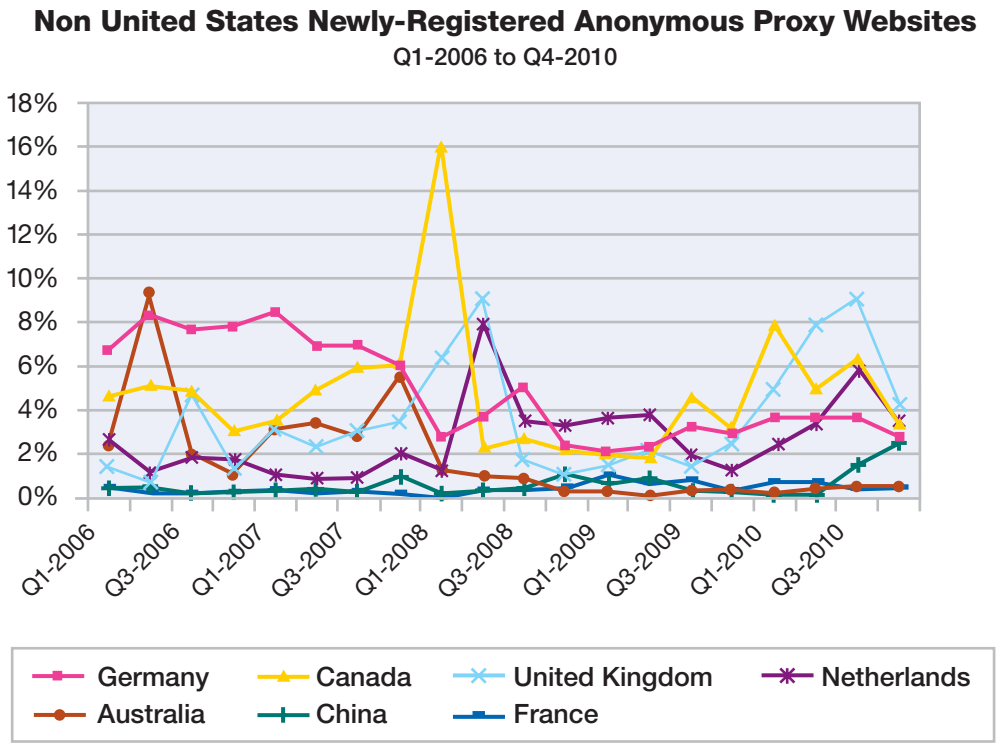

Figure 20: Non United States Newly-Registered Anonymous Proxy Websites – Q1-2006 to Q4-2010

Malicious websites

This section discusses the countries responsible for hosting the malicious links along with the types of websites that most often link back to these malicious websites. Exploits from Malicious websites discusses the web exploit toolkits involved in the majority of these malicious websites.

Geographical location of malicious web links

The United States continues to reign as the top hosting country for malicious links. More than one third of all malware links are hosted in the U.S. While China was on top two years ago, it is runner-up in 2010, hosting 8.5 percent—only 0.2 percent more than France. Romania is new within these top malicious URL hosting countries, claiming 7.9 percent (as shown in Figure 21).

The second-tier countries have also shifted, and, most significantly, many more countries seem to be jumping into the game.

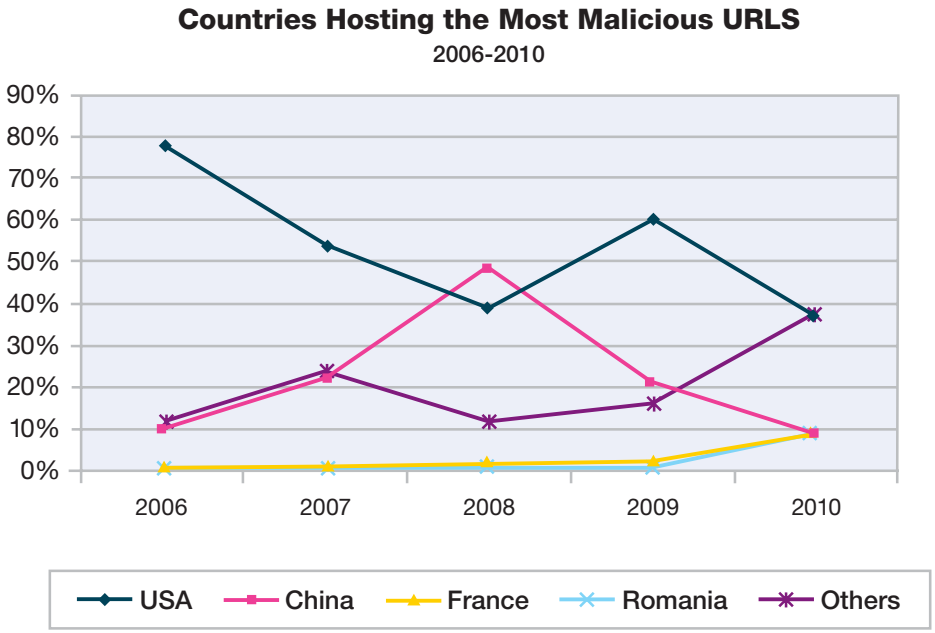

Figure 21: Countries Hosting the Most Malicious URLS – 2006-2010

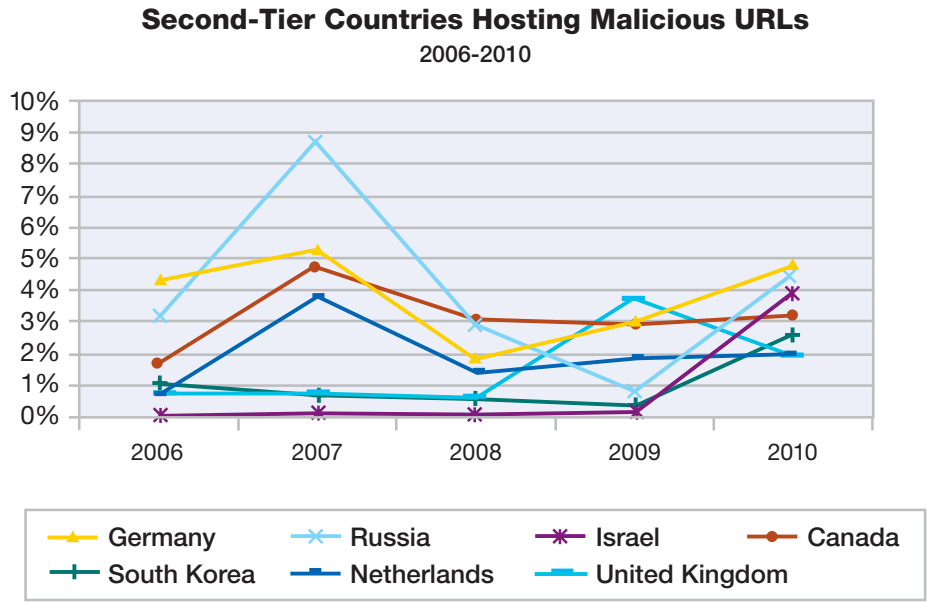

Figure 22: Second-Tier Countries Hosting Malicious URLs – 2006-2010

Good websites with bad links

As described in Web Application Vulnerabilities and Common Domains in URL Spam, attackers are focusing more and more on using the good name of trusted websites to lower the guard of end users and attempt to obfuscate their attacks with protection technologies. The use of malicious web content is no different. The following analysis provides a glimpse into the types of websites that most frequently contain links to known, malicious links.

Some of the top categories might not be surprising. For example, one might expect pornography and gambling to top the list. Indeed, together they own more than 30 percent of all malicious links. However, the second -tier candidates fall into the more "trusted" category.

Blogs, bulletin boards, search engines, personal websites, shopping sites, education, online magazines, and news sites fall into this second-tier "trusted" category. Many of these websites allow users to upload content or design their own website, such as personal content on a university's website or comments about a purchase on a shopping website. It is unlikely that these types of websites are intentionally hosting malicious links. The distribution is probably more representative of the types of websites that attackers like to frequent in hopes of finding a loop-hole (like a vulnerability or an area that allows user-supplied content) in which they can incorporate malicious links in hopes of compromising an unsuspecting victim.

The chart below lists the most common types of websites that host at least one link that points back to a known malicious website.

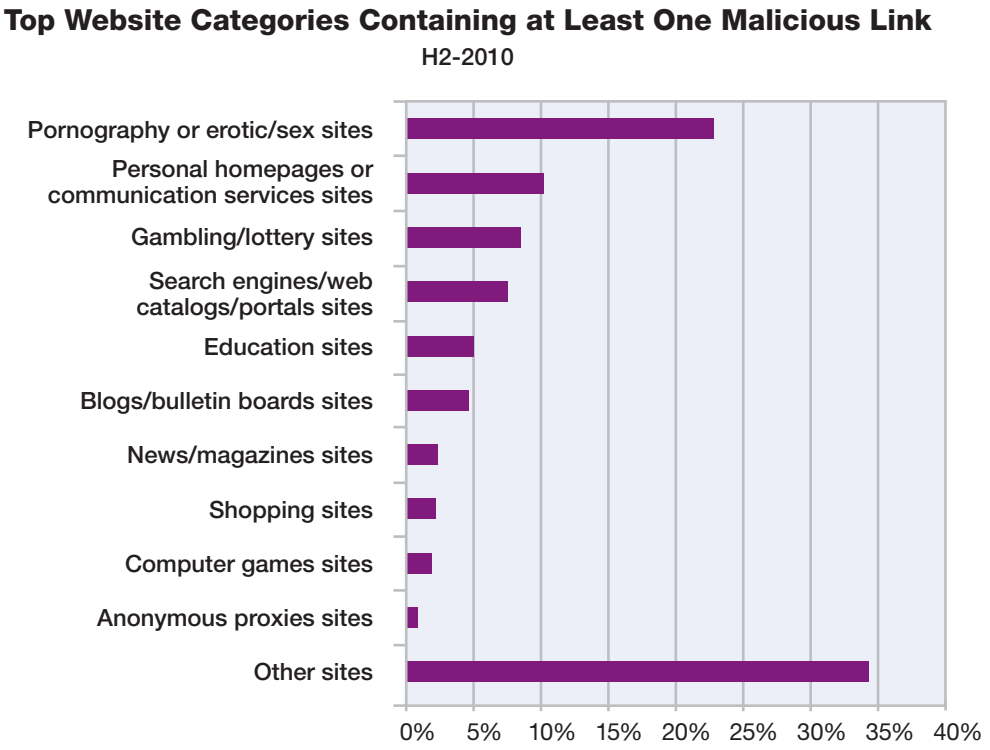

Figure 23: Top Website Categories Containing at Least One Malicious Link – H2-2010

When comparing this data with the data of the previous years, interesting trends appear. Particularly in the first half of 2010, professional "bad" websites like pornography or gambling websites have increased their links to malware, making it appear more likely that "professionals" are improving their efforts to systematically distribute their malware. However, in the second term of 2010 they declined again, but both end in a percentage above the levels of 2009.

Educational sites such as university websites have also seen increases in malware links since 2009. The same is true for Blogs and bulletin boards until mid-2010. Then they significantly decreased and fell below 5 percent for the first time in more than a year. Moreover, we noticed increases for computer games and anonymous proxy sites, but on a lesser level.

The only major category that did not decrease significantly in the second half of 2010 was gambling sites.

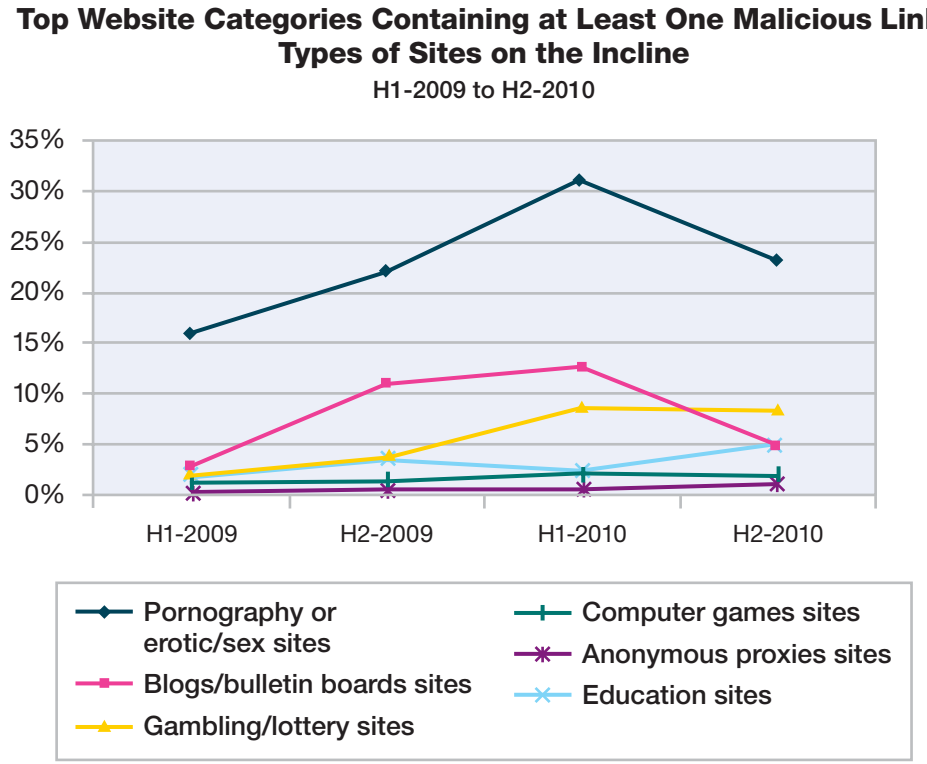

Figure 24: Top Website Categories Containing at Least One Malicious Link: Types of Sites on the Incline – H1-2009 to H2-2010

Personal homepages are no longer the most prevalent category that host at least one malicious link. Personal homepages have improved—they now host less malicious links—compared to the first half of 2009. One reason may be that personal homepages are more out of style in favor of web 2.0 applications such as profiles in social or business networks. Search engines, portals, shopping sites, and news sites have also improved or stayed on a low level. These traditional legitimate interactive sites have been used to exchange information and opinions for years. Thus, it is likely that providers of those services have increased their efforts in IT security.

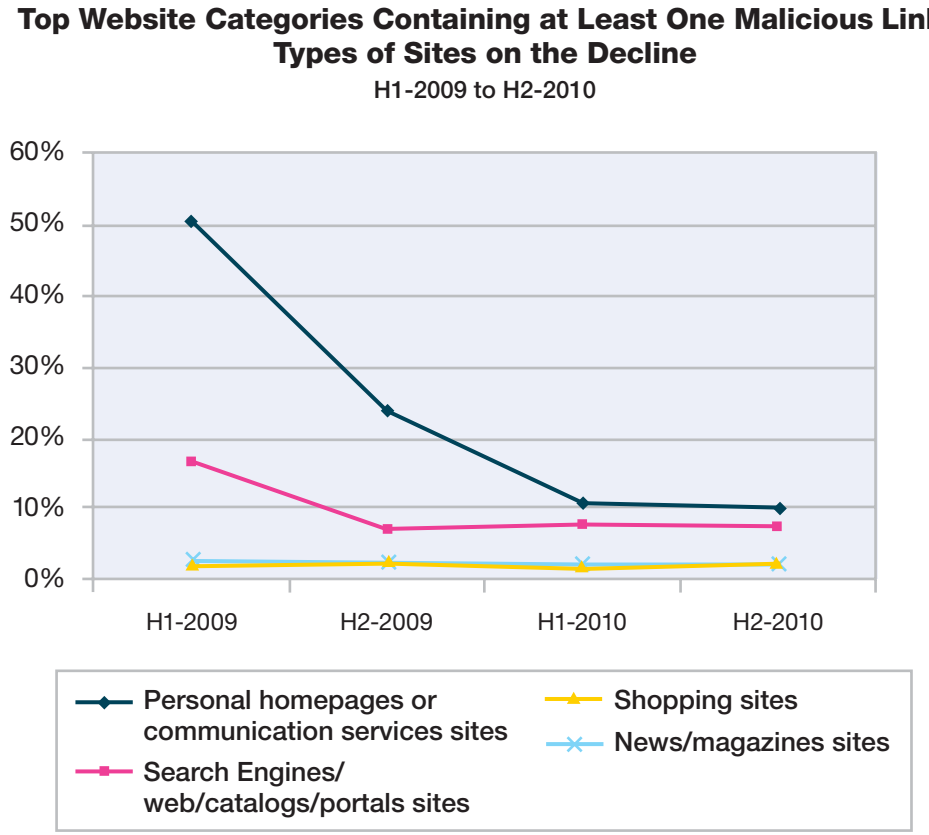

Figure 25: Top Website Categories Containing at Least One Malicious Link: Types of Sites on the Decline – H1-2009 to H2-2010

Until now we have not consider the number of malicious links placed on a website. The difference might be:

- When hosting only one or two malicious links on a site, the owner of the site might not understand or know that the link is bad – there is no ill intent.
- When placing ten or more links on a site, then this is done systematically and intentionally to get visitors clicking on bad links. The goal of the owner might be to enjoy a financial advantage from the compromises.

Out of the categories of websites that host 10 or more of these links, pornography accounts for nearly 30 percent and gambling accounts for nearly 29 percent.

Compared to the data six months ago, the values in most categories have stayed flat or slightly decreased but gambling increased by nearly one percent. Against the background of 0.6 percent of the adult population having problem gambling issues (see **http://en.wikipedia.org/wiki/Gambling_addiction#Prevalence**), gambling sites are a popular target for malware distributors. Note also that Personal Homepages and Communication Services increased by 1.7 percent and Educational sites increased by 0.6 percent.

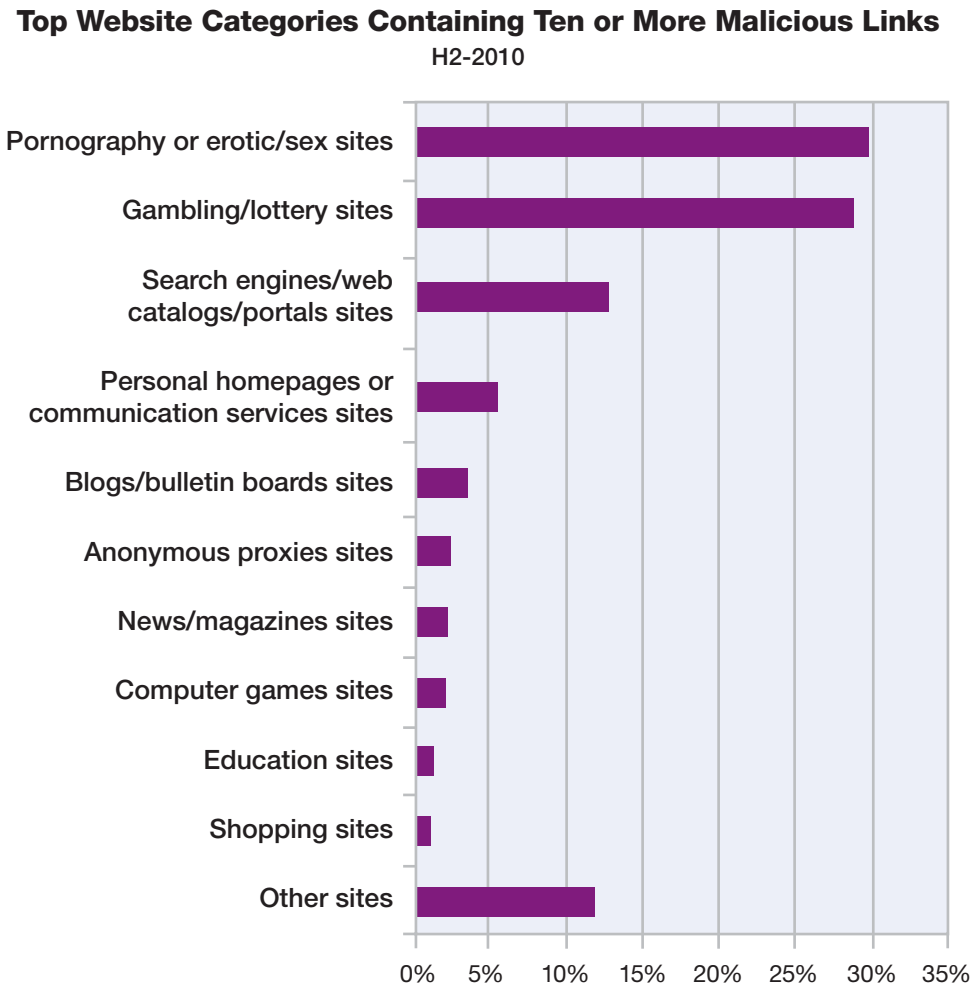

Figure 26: Top Website Categories Containing Ten or More Malicious Links – H2-2010

Spammers focus on content rather than volume

The IBM spam and URL filter database provides a world-encompassing view of spam and phishing attacks. With millions of email addresses being actively monitored, the content team has identified numerous advances in the spam and phishing technologies attackers use.

Currently, the spam filter database contains more than 40 million relevant spam signatures. Each piece of spam is broken into several logical parts (sentences, paragraphs, etc.). A unique 128-bit signature is computed for each part and for millions of spam URLs. Each day there are approximately one million new, updated, or deleted signatures for the spam filter database.

This section addresses the following topics:

- Major content trends in spam 2010
- Most popular domains and top level domains used in spam
- Spam country[9] of origin trends, including spam web pages (URLs)
- Most popular subject lines of spam

9 The statistics in this report for spam, phishing, and URLs use the IP-to-Country Database provided by WebHosting.Info (http://www.webhosting.info), available from http://ip-to-country.webhosting.info. The geographical distribution was determined by requesting the IP addresses of the hosts (in the case of the content distribution) or of the sending mail server (in the case of spam and phishing) to the IP-to-Country Database.

Major content trends in spam for 2010

After the last major threats of image-based and PDF spam in 2007, we did not see major changes in the content of the spams in 2008 and 2009, apart from another short-period threat of image spams in the first term of 2009. One characteristic for the low changes in technical spam content was the constant level of HTML-based spam (in most cases a bit more than 80 percent) and plain-text spam (mostly 10-15 percent).

In 2010 there were major changes in the technical content of spam. To see these trends at a glance, see Figure 27.

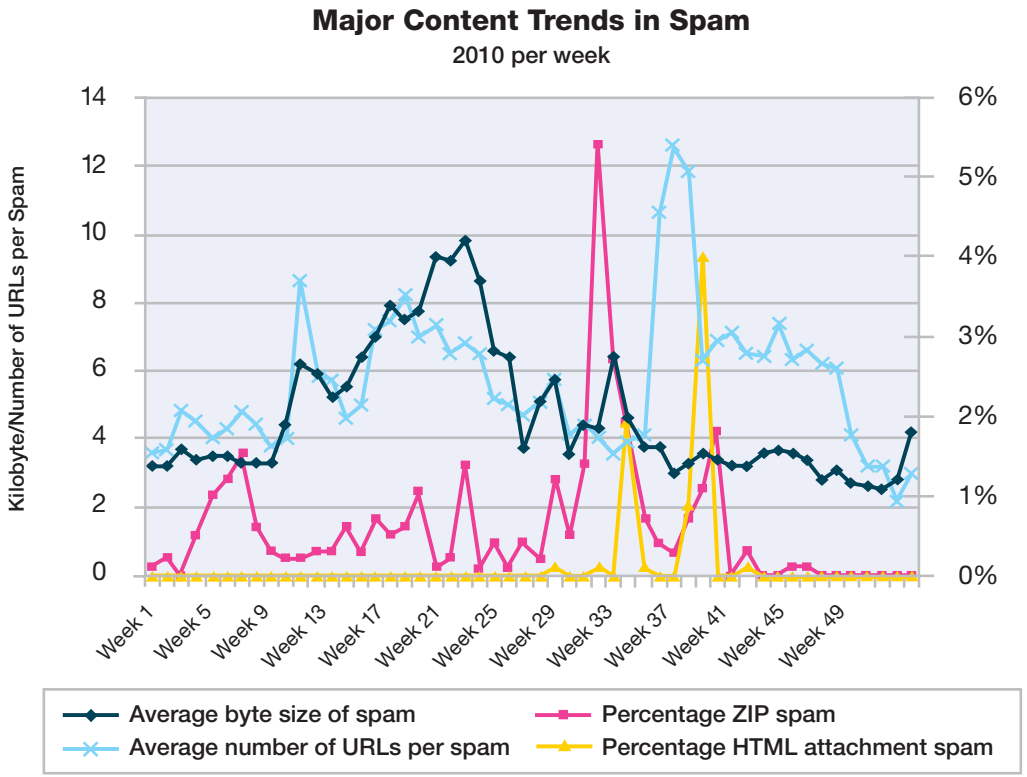

Figure 27: Major Content Trends in Spam – 2010 per week

Let's have a closer look at the trends and the characteristics:

- **March-August:** Random text spam combined with random URLs, significantly increased the average byte size of spam. In previous years the average byte size of spam was directly dependent on the percentage of image-based spam. But in 2010 the percentage of image spam was flat and below two percent (in most cases below one percent). When looking at these larger spams one can see large text fragments randomly chosen from the Internet, complemented by random URLs (syntactically correct URLs build from random characters or words, but many of them do not exist in the Internet). Random text is a very old technique of the spammers to make spam look more legitimate. However, recent anti-spam techniques do not have any problems with it. So why did spammers re-activate this old approach? Maybe they hoped that those masses of text would confuse Bayesian classifiers, particularly self-trained Bayesian classifiers, which are used in a non-business context; hence, these spam attacks might be targeted to these non-business users.
- **August—Spam with malicious ZIP attachments:** At the beginning of August, spammers began sending spam threats with ZIP attachments. We looked into these messages, and each ZIP file contained a single EXE file that was malicious. Spammers used different kinds of malware, e.g. variants of the Zeus Trojan or a copy of the Bredolab downloader (see sidebars). More details on these spam threats with ZIP attachments can be found at **http://blogs.iss.net/archive/ZIPMalwareSpam.html**. IBM Proventia customers can use the Email_Zip_Executable_Content signature to detect threats like these. The spammers used typical methods to attract the user's attention by using subjects such as:
  - Your Flight Ticket
  - Financial Summary
  - Statement Notification
  - Financials
  - FW: Car & Car loan
  - Employee Orientation report

Zeus Trojan

Zeus is a very common Trojan that's generated with a kit that anyone can purchase online. There are many different individuals and groups that have Zeus botnets set up. There are a lot of ways it gets spread, but the operators of this particular botnet are growing it by sending out emails with ZIP file attachments. The goal of Zeus botnets is usually to steal personal information, and the type of information stolen is commonly online banking data that criminals can use to access bank accounts to transfer money. For more information about the Zeus botnet see Trojan Bot networks in the section **"IBM Managed Security Services—A global threat landscape".**

- **September—Spam with HTML attachments:** There are some similarities between the ZIP attachment spam emails of the month before and the HTML attachment spam. In both cases the user's computer gets infected when clicking on the attachment. Furthermore, in the HTML attachment spam, the user's attention is attracted in the same way as in the ZIP attachment spam by something in the email text body such as:
  - Please see attached invoice for Stockton floor project
  - More details are in the attached invitation
  - See attached for breakdown—the $40 HOA will not be included in payment do deduct from total which = $1095/mo
  - Please print out the invoice copy attached and collect the package at our office
  - Attached is a copy of the deposit received for your records
  - Here are the signed documents
  - memo on image secrecy (attached)
  - Enclosed is my CV for your consideration
  - You will find the resume attached to this email
  - Attached you will find the fall daily tour schedule for your review

- **September-November—Random URL spam:** During this time period, spammers did not use random text but instead used random URLs extensively. This resulted in more than 12 (syntactically correct but otherwise useless and random) URLs per spam on an average during the beginning weeks of this time period. In the following weeks, we recognized more than six URLs per spam, which is still above the normal levels of 2-4 URLs per spam on an average.

- **December—Increased average byte size of spam again:** This time, this is a result of the drop of the spam volume by 70 percent (**see section "Spammers on holiday at the end of the year" page 46**), that affected particularly small spam.

Against the trends of previous years—wherein spammers made very few changes in the technical content of spam throughout the year, in 2010, spammers made a continuous effort to change the technical contents regularly. In the next section, we will discuss an associated factor—the volume of spam.

Bredolab downloader

This Trojan downloads a rogue antivirus program called SecurityTool that pretends to find viruses on your PC when none exist.

Spam volume

While we recognized significant increases of the spam volume year over year until 2009, in 2010 there were a few months with ups and downs in the volume of spam seen over the year. However, the overall trends stayed flat, and we saw less volume at the end of the year in comparison to the beginning of 2010.

Conclusions about spam volume and content

Why are spammers making an effort to change the technical content of spam more often than in previous years but are no longer focusing on increasing the overall volume of spam? Here we ponder a few presumptions about these possible trends. Some trends might be more plausible than others.

- Perhaps in recent years there was a linear connection between the number of spam messages and the profit reached by spam. Is this connection lost?
- Is the spam market saturated? Will we even see a decrease of spam volume in the upcoming years?
- Since there is only one single point to combat current spam - when receiving them - for the companies (or the users), did the bad guys change their focus to other - more distributed - areas that are more complicated to take countermeasures? This assumption is strengthened by:
  - the increase of Botnet Trojan Activity in 2010 - see section **"Trojan Bot networks"**
  - the surge of Obfuscation Activity in 2010 - see section **"Obfuscation"**
  - the growth of Backscatter Activity in 2010 - see section **"Spoofed Denial of Service attacks"**
  - the rise of the Vulnerability Disclosures in 2010 - see section **"2010 - A record setting year"**
- Is the increase of spam messages only achieved within internal social network messaging systems and other Web 2.0 applications?
- Are spammers cautious in efforts with increasing the levels too much because the more similar spam messages they produce, the easier they can be detected and blocked by perfected spam filters? That would mean, they assume that they have reached an optimum concerning the spam volume.
- Are the new operating systems more secure and prevent a further increase of the levels?
- Do even "spamming companies" suffer from the war for talent, hence, they have recruitment problems?

It is very unlikely that the spam business has become unprofitable. One scenario could be that spam volume stays flat but the kinds of spam change more frequently to circumvent spam filters with new types of spam that are more difficult to detect.

Maybe there will be more experiments with other attachment types? We tallied the most popular file types, and there is one file type becoming more and more popular – Open Office documents. When do spammers use those attachments?

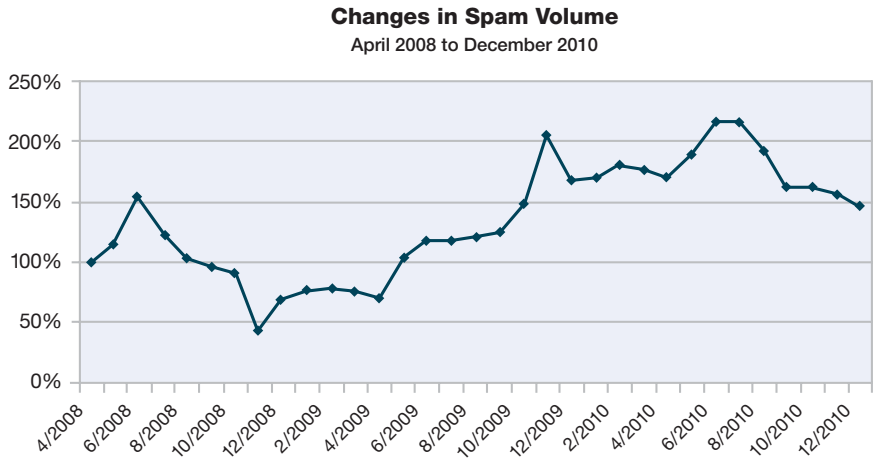

Figure 28: Changes in Spam Volume – April 2008 to December 2010

Spammers on holiday at the end of the year

One week before year's end, spammers surprised us by sending out 70 percent less spam than the weeks before; this period lasted about two and a half weeks. After the Christmas holiday season, spam levels returned to the same level as before Christmas.

When looking at the reductions of the spam volume per country there were some countries, such the U.S., Canada, and UK, with a decline of more than 90 percent. More about the declines per country and some more details can be found on **http://blogs.iss.net/archive/2011spambotdecline.html**.

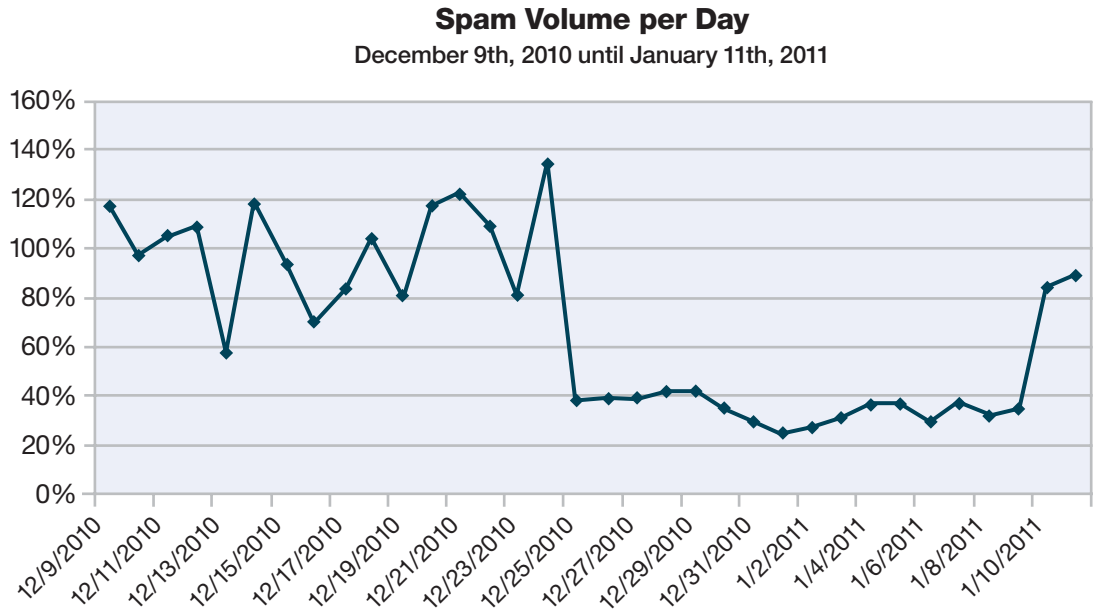

Figure 29: Spam Volume per Day – December 9th, 2010 until January 11th, 2011

Regional spam volume per day of the week

Another approach for looking at the spam volume is checking the spam volume per day of the week. If we received equal volumes each day, then we would receive 14.3 percent of the weekly spam volume per day. When looking at spam written in English, French, or Spanish, this appears more or less the case.

English spam is distributed very consistently over the week days. The days with the least amount of spam are Wednesday (14.0 percent) and Sunday (13.7 percent); the days of the week with the most spam are Tuesday (14.7 percent) and Friday (14.8 percent). The most French spam is received on Thursday (15.7 percent) and Friday (15.8 percent). The greatest spam day of the week for Spanish spam is Monday, when they process 18 percent of the weekly amount of their spam. However, the difference between the other week day amounts for French and Spanish is rather low.

The situation is different for Russian and Portuguese spam. On weekends, we receive much less spam written in these two languages. Almost 90 percent of spam in the Russian language is sent out on week days; on Saturday and Sunday, they only send out about five percent each day. Their strongest days are Tuesday, Wednesday, and Thursday, when they process about 20 percent of their weekly amount each day. The patterns are similar for Portuguese spam. Their strongest days are Tuesday to Thursday, and their weakest days are Saturday and Sunday.

Assuming that spammers prefer not to work weekends, it appears that spam in the English, French, and Spanish languages is sent out completely automatically, retaining its typical volume on weekends. Contrarily, Russian and Portuguese spam requires more manual work, resulting in a significant drop at the weekends.

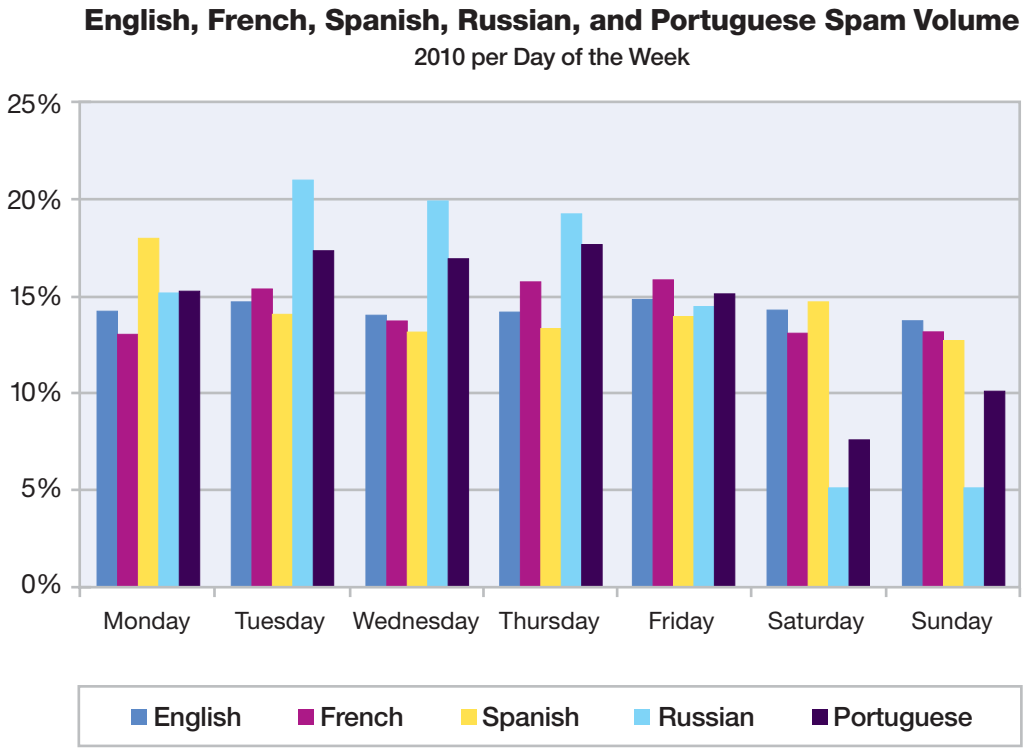

Figure 30: English, French, Spanish, Russian, and Portuguese Spam Volume – 2010 per Day of the Week

Common domains in URL spam

The vast majority of spam, more than 90 percent, is still classified as URL spam—spam messages that include URLs that a person clicks to view the spam contents. It is worthwhile to take a closer look at the most frequently used domain names in URL spam. The table on the following page shows the top 10 domains per month throughout 2010, with some key domains highlighted.

The majority of those domain names are well-known and trusted (highlighted in color in the table on page 49). Not only do these legitimate websites provide a recognizable (and trustworthy) web link to the end user, but spam messages using them may also successfully evade some anti-spam technology because they only use legitimate links in their spam emails. There are different types of well-known domains:

- **Internet service providers (blue):** Used by spammers in recent years to make look their spams appear trustworthy.
- **Image-hosting websites (green):** Also used by spammers for several years. Spammers like to vary between well known image-hosters like flickr.com and imageshack.us and many other small and medium-sized image-hosting websites.
- **Random word domains (orange):** From July to September 2010 spammers used random words to "build" URLs. This was done in such a massive way that the very common words "the", "of", "and", "in", "a" even made it to the top ten with the ".com" extension. Since then, we have seen random domains built from random characters and now it appears we see random domains built from random words.
- **Official websites of Pfizer and Rolex (yellow):** From September 2010 on, spammers used the official websites of Pfizer (pfizer.com, pfizerhelpfulanswers.com, viagra.com) and Rolex (rolex.com). Obviously, spammers include in their strategies that most spam filters do not use simple keyword search anymore and even assume that URLs from pfizer.com or rolex.com make their messages looking more legitimate.
- **URL shortening services (purple):** From September 2010 on, some of these services made it to the top 10.

The table of domains on the next page became more multicolored in the second half of 2010. That means that spammers used multiple methods to present their offers via URLs. This is another illustration of the move of spammers from volume to "content quality," as mentioned above.

Rank	January 2010	February 2010	March 2010	April 2010	May 2010	June 2010
1.	flickr.com	radikal.ru	livefilestore.com	livefilestore.com	imageshack.us	imageshack.us
2.	imageshack.us	imageshack.us	imageboo.com	imageshack.us	imageshost.ru	imageshost.ru
3.	radikal.ru	livefilestore.com	radikal.ru	imageshost.ru	myimg.de	pikucha.ru
4.	livefilestore.com	flickr.com	imageshack.us	imgur.com	xs.to	imgur.com
5.	webmd.com	live.com	googlegroups.com	myimg.de	imgur.com	mytasvir.com
6.	picsochka.ru	imageboo.com	live.com	xs.to	tinypic.com	mojoimage.com
7.	live.com	capalola.biz	akamaitech.net	icontact.com	livefilestore.com	myimg.de
8.	superbshore.com	feetorder.ru	gonestory.com	tinypic.com	icontact.com	twimg.com
9.	tumblr.com	laughexcite.ru	bestanswer.ru	live.com	googlegroups.com	icontact.com
10.	fairgreat.com	hismouth.ru	wrotelike.ru	binkyou.net	images-amazon.com	twitter.com

Rank	July 2010	August 2010	September 2010	October 2010	November 2010	December 2010
1.	imageshack.us	yahoo.com	the.com	businessinsider.com	rolex.com	pfizer.com
2.	icontact.com	the.com	of.com	migre.me	msn.com	viagra.com
3.	the.com	icontact.com	msn.com	4freeimagehost.com	bit.ly	msn.com
4.	myimg.de	feetspicy.com	pfizerhelpfulanswers.com	bit.ly	pfizer.com	rolex.com
5.	of.com	of.com	and.com	postimage.org	co.cc	bit.ly
6.	imgur.com	ratherwent.com	bit.ly	imgur.com	royalfoote.com	product45h.com
7.	by.ru	and.com	in.com	pfizer.com	royalbelie.com	newpfizermed5k.com
8.	and.com	facebook.com	yahoo.com	viagra.com	royalreleasable.com	xmages.net
9.	in.com	in.com	a.com	uploadgeek.com	luxurystorewatch.com	cordfork.com
10.	tastymighty.com	a.com	x-misc.com	vipplayerq.com	basincook.com	onlinepfizersoft2.com

Table 4: Most common domains in URL spam, 2010