IBM Global Technology Services
January 2009

IBM Internet Security Systems X-Force® 2008 Trend & Risk Report

Table of Contents

Overview

The IBM Internet Security Systems X-Force® research and development team discovers, analyzes, monitors and records a wide array of computer security threats and vulnerabilities. According to X-Force observations, many new and surprising trends surfaced throughout 2008. We hope that the information presented in this report about these trends will provide a foundation for planning your information security efforts in 2009 and beyond.

The security industry puts a lot of effort into the technical evaluation of security threats, examining, sometimes at great length, the potential threat that each issue might present to corporations and consumers. Criminal attackers out for profit, however, have considerations that the security industry does not always take into account, such as monetization cost and overall profitability.

There were a lot of headliner security issues in 2008, some of which never amounted to mass exploitation. The first section of this report, Exploitation Economics: What Didn't Happen in 2008 and Why on page 5, discusses this issue in detail and provides some lessons that can help our industry to better evaluate these types of security issues in the future.

Computer criminals are looking for information that they can quickly turn for a profit. By and large, this quick turn on investment means consumer credit card information and bank account access credentials. While sometimes attackers find ways to harvest vast amounts of this sort of data from corporate servers and networks, a great deal of this information is stolen by spyware running directly on end user PCs

Corporations with their advanced patching and protection mechanisms may also create more obstacles (higher monetization costs and lower profitability) for attackers. Consumers, on the other hand, with their lack of protection, casual patching behaviors, and general lack of security prowess remain easy targets. Clear indicators for this problem are the continued mass exploitation of browser issues, especially ActiveX controls. New exploitation vectors, like the use of PDF files and multimedia applications like Flash containing embedded exploits became much more prevalent than ever before with an uptick towards the end of the year.

Certain types of corporate applications, namely custom-built software like Web applications remain a highly-profitable and inexpensive target for criminal attackers. The sheer number of new vulnerabilities, the majority of which have no available patch, coupled with the hundreds of thousands of custom Web applications that are also vulnerable (but never subject to a vulnerability disclosure, much less a patch), have become the Achilles heel of corporate security. Attackers continue to target Web application vulnerabilities, especially SQL injection, to plant malware on unsuspecting users that visit vulnerable Websites.

2008 Highlights

Vulnerabilities

- *2008 proved to be the busiest year in X-Force history chronicling vulnerabilities – a 13.5 percent increase compared to 2007.*
- *The overall severity of vulnerabilities increased, with high and critical severity vulnerabilities up 15.3 percent and medium severity vulnerabilities up 67.5 percent.*
- *Similar to 2007, nearly 92 percent of 2008 vulnerabilities can be exploited remotely.*
- *Of all the vulnerabilities disclosed in 2008, only 47 percent can be corrected through vendor patches. Vendors do not always go back to patch previous year's vulnerabilities. 46 percent of vulnerabilities from 2006 and 44 percent from 2007 were still left with no available patch at the end of 2008.*
- *The two largest categories of vulnerabilities in 2008 are Web application at 55 percent and vulnerabilities affecting PC software at roughly 20 percent.*
- *For vulnerable operating systems, operating systems from Apple and the base Linux kernel have dominated the top spots for vulnerability disclosures over the past three years.*

Web-Related Security Threats

- *The number of new malicious Web sites in the fourth quarter of 2008 alone surpassed the number seen in the entirety of 2007 by 50 percent. Last year, China replaced the US as the most prolific host of malicious Web sites.*
- *Even good Web sites are facing more issues. Web applications, in particular, are increasingly vulnerable and highly profitable targets for helping the criminal underground build botnet armies*
- *Spammers are turning to the Web. URL spam (a spam email with little more than a link to a Web page that delivers the spam message) took the lead as the main type of Spam this year, and Spammers more and more are using familiar domain names like news and blogging Web sites to host their content.*
- *Web applications in general have become the Achilles heel of Corporate IT Security. Nearly 55% of all vulnerability disclosures in 2008 affect Web applications, and this number does not include custom-developed Web applications (only off-the-shelf packages). 74 percent of all Web application vulnerabilities disclosed in 2008 had no available patch to fix them by the end of 2008.*
- *Last year, SQL injection jumped 134 percent and replaced cross-site scripting as the predominant type of Web application vulnerability.*
- *Exploitation of Websites vulnerable to SQL injection has increased from an average of a few thousand per day, when they first took hold early in 2008, to several hundred thousand per day at the end of 2008.*
- *In addition to these vulnerabilities, many Web sites request the use of known vulnerable ActiveX controls, which leave Web site visitors who do not have updated browsers in a compromised position.*
- *Although the number of vulnerabilities affecting Web browsers went down in comparison to 2007, they continue to be the main target of exploitation. New categories of threats affecting clients are on the rise, specifically in the areas of malicious documents, multimedia applications, and potentially Java applications which are easy to host on the Web.*

Spam and Phishing

- *The McColo shutdown had the most impact on spam activity in 2008, not only affecting quantity but also affecting the type of spam sent and the countries that most frequently sent it.*
- *Although the volume of spam dropped after the shutdown, X-Force expects it to return to normal by the first quarter of 2009.*
- *Simple spam (text or URL-based) replaced complex (PDF, image, etc.) spam in 2008, with a focus on URL spam near the end of the year. Spammers increasingly use familiar URL domains, like blogging Websites and news Websites, to host spam messages.*
- *Although most of the spam URLs use the .com TLD (top level domain), a steady increase in the use of .cn is evident, and, when it comes to malicious URLs, the number of malicious URLs hosted in China surpassed that of the US this year.*
- *More than 97 percent of Spam URLs are up for one week or less.*
- *In terms of the servers sending spam, Russia surpassed the US in 2008, and was accountable for 12 percent of all spam sent last year.*
- *The most popular subject lines of phishing and spam are not so popular anymore. The top ten subject lines of 2008 took up a much smaller percentage in comparison to 2007. Spammers and phishers alike are becoming more granular and targeted, working harder in essence, to reach more targets. In 2007, the most popular phishing subject lines represented about 40% of all phishing emails. In 2008, the most popular subject lines made up only 6.23% of all phishing subject lines.*
- *Another trend that developed in 2008 is the focus on user action. Rather than having a generic subject like "security alert," phishers attempt to engage the user into doing something, like fixing an account that has been suspended or updating their account information.*
- *The majority of phishing – nearly 90 percent – was targeted at financial institutions. Over 99% of all financial phishing targets are in North America or Europe, with the majority of targets in North America (58.4 percent).*

Malware

- *46 percent of all malware collected over 2008 were Trojans. Trojans targeting users of online games (Onlinegames, Magania) and online banking (Banker and Banload) remain prevalent for the whole year; which indicates that these specific user groups are highly targeted in 2008.*

Exploitation Economics: What Didn't Happen in 2008 and Why

"Amateurs Study Cryptography; Professionals Study Economics" is the snarky title of one of the chapters in the recently published "New School of Information Security" by Adam Shostack and Andrew Stewart. This chapter title highlights a blind spot that presently plagues some corners of the security industry. Of course, there are many serious professionals making important contributions through a better understanding of the technical nature of computer security problems, but there is not enough focus on the way that economic incentives and externalities interact with those technical problems.

When we fail to consider the economic context in which computer security vulnerabilities exist, we end up prioritizing the wrong threats. As X-Force has looked back over the highly-publicized vulnerabilities of 2008, we have noticed that a number of the critical threats did not materialize into widespread attacks in the field. A closer look at those threats reveals some lessons that can help our industry to better evaluate future security issues.

Business Analysis of Computer Security Threats

Presently, the security industry prioritizes threats almost entirely on the basis of technical measures of the risks that they present. The Common Vulnerability Scoring System (CVSS) is the industry-standard threat prioritization system. The metrics that it considers for its base scores focus on the technical aspects of the vulnerability. They consider:

- *Level of difficulty in accessing the vulnerable software interface*
- *Impact that a successful attack has on the confidentiality, integrity, and availability of vulnerable systems*
- *Public availability and reliability of exploit code*
- *Availability of patches or workarounds*

Although some economic considerations are included in the environmental factors of CVSS, those factors are considered to be unique to each enterprise, and they are not incorporated into the CVSS base scores that appear in industry security vulnerability databases. Furthermore, those economic considerations are focused entirely on the cost that a successful attack could pose to an organization.

While all of the factors considered by CVSS are important, what CVSS scores fail to capture is the economic opportunity that a vulnerability presents to an attacker. The days of amateurs, college students, or hackers taking joy rides on corporate information systems are largely over. Today's attackers are economically motivated. They are international criminal organizations who make a living stealing financial information and identities. Today's threat is far more sophisticated and far more dangerous than the security threats of yore, but in some ways it is more predictable. Whereas an amateur hacker might take an interest in any security vulnerability that comes along, serious computer criminals are particularly interested in vulnerabilities that provide a significant return on investment.

CVSS scores fail to capture the economic opportunity vulnerabilities present to attackers.

The result of this new reality is that there have been several vulnerabilities this year that received very high CVSS scores and raised widespread alarm within the security industry. However, they were not widely exploited in the wild. In most cases, these vulnerabilities did not fit well into the current business models of computer criminals. IT departments should not ignore vulnerabilities that present serious risks to their infrastructure simply because they feel those vulnerabilities will not become widely popular with organized crime. Highly sophisticated adversaries may use rarely-exploited vulnerabilities in targeted attacks. However, more careful consideration of the way that vulnerabilities fit into the business models of criminal organizations will help better prioritize IT protection and patching efforts.

Criminal Economics 101

On a basic microeconomic level, an understanding of the opportunity for a computer criminal comes from considering the amount of revenue that can be generated from exploiting a vulnerability relative to the cost of doing so. Obviously, vulnerabilities that present a high revenue opportunity at a low cost are likely to be popular with attackers. Both revenue (opportunity) and cost are made up of a complicated set of components, and some of these components can be influenced by the security industry.

Criminal Opportunities

The actual revenue that can be generated from exploiting a vulnerability is a combination of the size of the installed base of vulnerable hosts and the value to an attacker of controlling each host, usually due to the information the hosts contain and the price the attacker can ask for that information on the black market. When a vulnerability is first disclosed, the installed base of vulnerable hosts may be quite large, and if the value of controlling those hosts is also large, the attacker has a significant theoretical revenue opportunity. This sort of situation may motivate efforts by the security industry to roll patches out quickly and reduce the size of the installed base. If the industry is effective, the total real revenue opportunity may become too small for attacks to materialize. On the other hand, there may be cases where the installed base of vulnerable hosts is large, but the value of controlling the type of host that typically runs the vulnerable software is small, and so attackers have little incentive to exploit the vulnerability regardless of what the security industry does to remediate it.

Criminal Costs

The cost of generating revenue from exploiting vulnerabilities is also made up of a number of factors. Two aspects of the cost that CVSS captures well are the cost of obtaining an exploit, which depends on whether or not an exploit is publicly available, and the difficultly associated with using it. CVSS also captures the impact of the exploit – what does the attacker get – in technical terms. However, a financially motivated attacker has to turn whatever access or performance degradation has been caused by the attack into money. Some kinds of access are more expensive to monetize than others.

As is the case with legitimate businesses, criminal organizations have operational processes that are built up around repeatable sets of circumstances and automatable tasks. Vulnerabilities that fit into existing processes and which can leverage existing automation are easy for criminals to monetize. Vulnerabilities that require the development of new processes or software are much less likely to present an attractive opportunity to criminals, particularly if they represent a one-of-a-kind set of circumstances that is unlikely to be repeated in the future. Even when it does make sense for criminals to develop a new attack methodology to exploit a new class of vulnerabilities, widespread attacks will usually take longer to emerge than for vulnerabilities that fit directly into an existing process.

Examples

To get a better understanding of how these factors affect exploitation lets consider a few of the big vulnerability disclosures from 2008. It first makes sense to consider a vulnerability that was widely exploited.

Microsoft Snapshot Viewer ActiveX Control Remote Code Execution

The Microsoft Snapshot Viewer ActiveX Control vulnerability (CVE-2008-2463) was assigned a CVSS base score of 7.5 by NIST. It was first reported to the public by Microsoft on July 7th, 2008 when they received word of targeted exploitation in the wild. Unfortunately, this vulnerability is easy to reliably exploit, as it's not a buffer overflow requiring the use of version specific offsets, but rather an interface that allows an arbitrary file to be downloaded from the Internet and placed anywhere on the victim's computer, including the startup folder or in place of a system file.

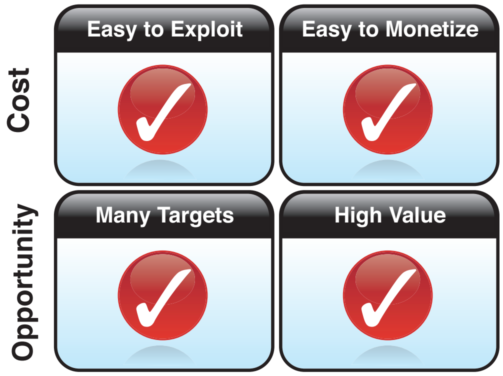


Figure 1: Exploitation Probability for Snapshot Viewer Vulnerability

By July 10th, an exploit for the vulnerability had already been incorporated into Web exploit toolkits, including NeoSploit. These toolkits are used by criminal organizations to automate the task of infecting a computer. When victim PCs stumble into the wrong Web page they are redirected to a server hosting the toolkit, which will automatically collect browser and other version information from the victim host and transmit an exploit to the victim's browser that will work against the software that the victim is running.

One problem with ActiveX controls is that sometimes they do not have to be installed on the target's computer for an attacker to take advantage of them. It is commonplace for a Web server to instruct a browser to download new ActiveX controls when the required control is not already installed. So, all an attacker has to do is entice the user's browser to install a vulnerable control, and then direct the browser to an exploit for that control once it has been installed. In this case the Snapshot Viewer control was signed with a Microsoft digital certificate. For an end user, seeing a prompt to install something new becomes much less suspicious when it appears as if it's coming from an entity you trust.

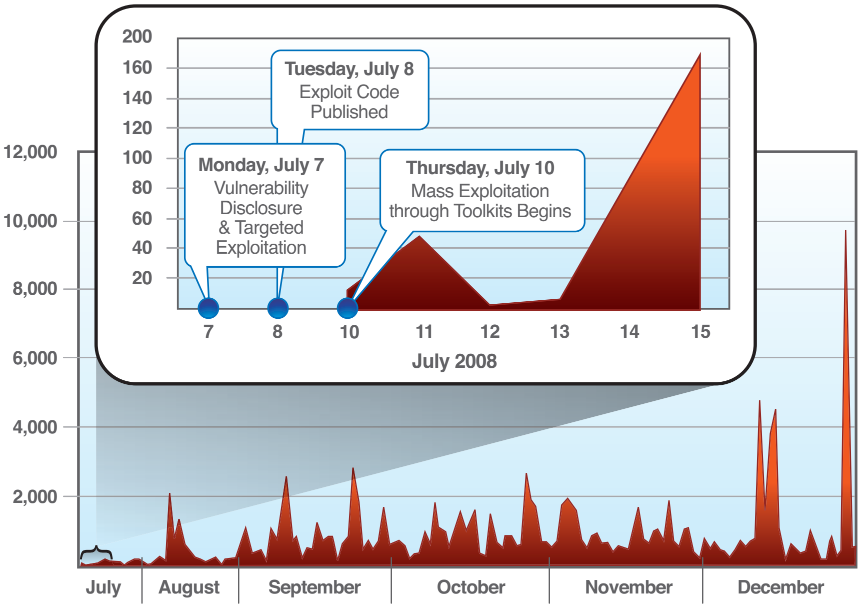


Figure 2: Microsoft Snapshot Viewer ActiveX Control Exploitation

By July 24th, IBM was tracking over 50 hosts actively exploiting the issue. By August 1st, new variants were reported which forced users who did not have the vulnerable ActiveX control to install it and then access the exploit, massively expanding the installed base of potentially vulnerable machines. Microsoft released patches for the vulnerability on August 12th.

The Snapshot Viewer vulnerability was popular with attackers not just because it was easy to exploit, but because it fit directly into established processes and software tools that computer criminals employ. Vulnerabilities are frequently reported in ActiveX controls and attackers are used to incorporating exploits into Web exploit toolkits and using them to propagate spyware that collects financial credentials. So in this case, the exploitation cost was low and so was the monetization cost. The installed base was essentially infinite, since the attackers could push down the Microsoft-signed control to anyone that would allow it to be installed. The bottom line is that a large revenue opportunity combined with a low monetization cost lead to a large amount of exploitation that still shows no sign of slowing down as shown in Figure 2. For more information about ActiveX exploitation and client-side vulnerabilities on the horizon, see Browser and Other Client-Side Vulnerabilities and Exploits on page 41.

SNMPv3 HMAC Security Bypass

Contrast the Snapshot Viewer vulnerability with the SNMPv3 HMAC Authentication Vulnerability (CVE-2008-0960). Originally, NIST assigned this vulnerability a CVSS base score of 6.8, causing it to be overlooked by many security analysts. Later, the score was revised to 10 when the full implications became clear. This vulnerability is very easy to exploit, requiring just 256 packets to access any password protected SNMPv3 interface. Also, sample exploit code can be downloaded from the Internet. The security consequences can be significant depending on what SNMPv3 has been configured to do. Of particular concern are Internet routers, which attackers may be able to reconfigure using this interface to disrupt, spy on, or modify Internet traffic. Given how powerful this vulnerability is, how easy it is to exploit, and how large the installed base is for SNMP, one would expect to see widespread exploitation, or at least probing and attempts at exploitation, but very little has materialized.

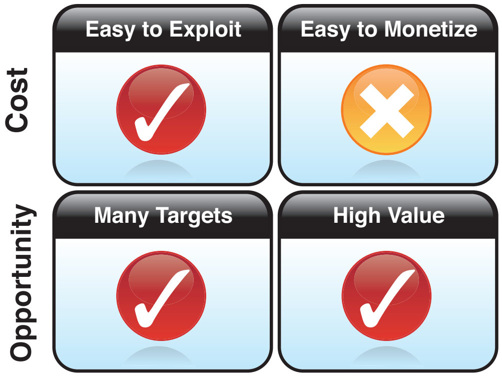


Figure 3: Exploitation Probability for HMAC Security Bypass

The reason is that even though this vulnerability is easy to exploit, successful attacks are difficult to monetize. This sort of vulnerability is a special case that does not fit easily into the business models of organized criminal groups who are attempting to profit from computer security problems. A real attack aimed at collecting financial information using this vulnerability would have two stages. The first stage involves reconfiguring a router to forward traffic through a network controlled by an attacker. However, because most financial transactions over the Internet are encrypted, a second stage is required, in which the attacker manipulates certain network traffic, such as DNS, in order to direct the victim to phishing sites under the attackers control, or in order to coax the victim to download malware. Ultimately, this sort of attack is very complicated, involving the development of a set of techniques and software that are specifically designed to leverage this sort of vulnerability. As patches are now available, the window of opportunity for exploiting this vulnerability is closing, so we have a very high cost of monetization coupled with a shrinking revenue opportunity. The result is little to no exploitation.

Microsoft IIS HTML Encoded ASP Remote Code Execution

There are some cases that might have gone either way. In February, Microsoft patched a remote code execution vulnerability in ASP (CVE-2008-0075) which also had a CVSS score of 10. This attack provides complete control over a vulnerable Web server, something computer criminals are very interested in, as they can redirect users to their exploit toolkits. An exploit in CORE IMPACT demonstrates that the vulnerability is exploitable, and a public analysis of the bug by H.D. Moore provides some technical details. However, no public exploit has ever emerged, and as of this publication X-Force is not aware of any private exploits being used in attacks.

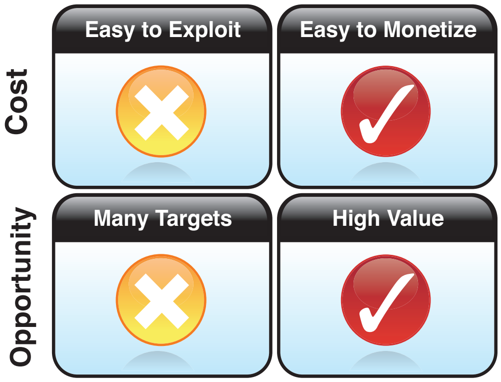


Figure 4: Exploitation Probability for Microsoft IIS HTML Encoded ASP

Perhaps the reason that no public exploit was ever developed for this vulnerability is that SQL injection is far too effective as a technique for exploit development to have been worth the effort. Many Websites developed in all kinds of languages are vulnerable to SQL injection, and they have been abused widely this year to inject JavaScript redirectors into Web pages that send unsuspecting victims into the waiting arms of browser exploit toolkits. The rise in exploitation is described in Active Exploitation & Automated SQL Injection Attacks in 2008 on page 36.

In contrast, this vulnerability provides a more limited opportunity, only working against ASP pages that are designed to accept Unicode formatted input and there is also some character filtering in play here that can frustrate code execution. Ultimately, a low revenue opportunity and a high exploit development cost makes this attack unattractive next to widespread SQL injection vulnerabilities that are very easy to exploit.

Microsoft Windows Server Service Remote Code Execution

Microsoft's Server Service vulnerability (CVE-2008-4250) is also worthy of consideration. This vulnerability was also scored at CVSS base 10, and rightly so as a worm (Gimmiv) was exploiting it in a limited fashion prior to its public disclosure. Obviously, the financial opportunity here for bad guys was huge, and the public disclosure of several iterations of proof-of-concept exploit code made exploitation easy. In fact, there were even reports of automated exploit generation tools for this vulnerability.

In years past, similar Microsoft RPC vulnerabilities have led to worm outbreaks that propagated very rapidly. For example, in the summer of 2003 the Blaster worm began exploiting an RPC DCOM vulnerability about a month after it was patched. According to research from the time, Blaster reached its propagation peak within 8 hours of its initial release. The Conficker worm exploiting the Server Service vulnerability has followed a different pattern. It was first reported in late November, also about a month after the initial patch release, but it spread very slowly. The worm didn't fully hit it's stride until January, and by then new variants were on the loose which employed multiple propagation methods, such as SMB share password cracking.

Blame for the success of the Conficker worm has largely been laid at the feet of a small portion of enterprises (reportedly about 3 in 10) who have turned off automatic Windows Update and operate very long compatibility testing cycles before rolling out security patches. According to reports, most consumers were patched quickly, and enterprises certainly had time to deploy patches, IPS signatures, or both. These factors contributed to the slow propagation of the worm relative to previous experiences. In fact, if it were not for the addition of secondary propagation methods (network shares, password cracking, and removable media which are all easily accessible in corporate environments), this worm may not have become very widespread at all.

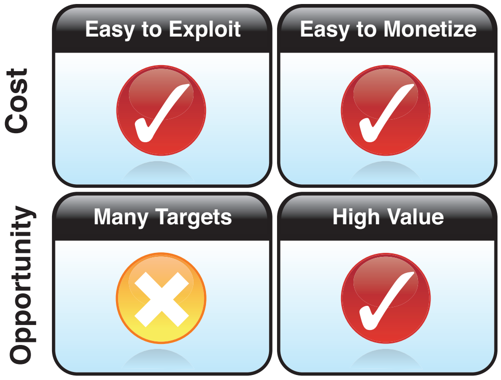


Figure 5: Exploitation Probability for Microsoft Windows Server Service

While critical, wormable vulnerabilities are still discovered, large worm outbreaks like Conficker are far less common than they were a few years ago. When they do happen, they happen more slowly, which is a testament to the efforts that have been made in the past few years across the IT industry to improve vulnerability response and overall computer security. However, the ultimate success of Conficker is evidence that we still have more work to do.

DNS Cache Poisoning

This brings us to the biggest computer security story of 2008: the DNS Cache poisoning vulnerability discovered by Dan Kaminksy (CVE-2008-1447). NIST gave this one a CVSS Base score of 7.5, but the widespread media attention this vulnerability received makes it clear that the computer industry saw this as a very serious threat. A massive effort was undertaken to upgrade the Internet's DNS infrastructure, but, according to a study performed by The Measurement Factory, a quarter of all DNS servers were still vulnerable as of October. Different DNS servers serve different-sized user populations, but one would expect a quarter of all DNS servers to represent a large enough group of potential victims that they would make an attractive target, and as public exploits are available, the attack is not terribly difficult to pull off. However, we are seeing very few real attacks in the wild. There are only a couple of anecdotes that we are aware of.

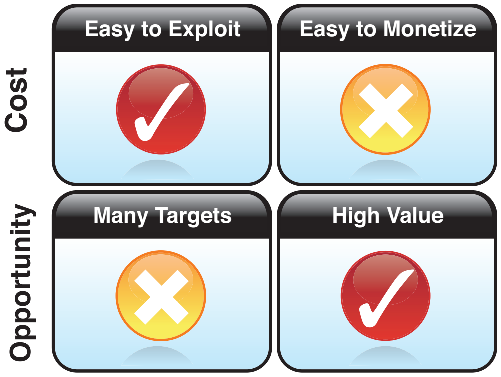


Figure 6: Exploitation Probability for DNS Cache Poisoning

Why? The first question to ask is whether this attack fits well into an existing criminal enterprise. At first glance the answer is yes. For the past few years, a Trojan known as DNSChanger or Zlob has infected victims by masquerading as a video codec. Among other things, this Trojan updates the victim's DNS server settings with IP addresses controlled by the attacker, redirecting certain traffic, including search results, to alternate destinations of the attacker's choosing. The attacker monetizes this control by selling the misdirected eyeballs to advertisers. Newer iterations of this Trojan released this year have become very sophisticated, updating the DNS settings in unsecured SOHO routers, and offering DHCP services, along with the rogue DNS server settings, on the infected computer's local LAN. The DNS Cache poisoning attack seems a natural compliment to this business model. This particular operation already has customers lined up to pay for it, and serves as an example that others might copycat.

However, there are a few important differences. Running a large-scale Internet scanning operation to seek out vulnerable DNS servers and systematically update their cache contents in order to direct large amounts of traffic to paying advertisers is a significantly different operational process from that which is presently employed by this group. They are currently focused on maintaining their Trojan software code and operating a few rogue DNS servers. Our perspective is that it takes time for criminal operations to decide to adopt an entirely new operational process like this, and to develop confidence with its use. They have to put thought into how to approach it and they have to spend time developing tools. For example, SQL injection vulnerabilities have been understood for nearly 10 years, but as we detail later in this report, it has only been in the last 12 months that large-scale automated exploitation of those vulnerabilities has begun. The state of SQL injection is not due to lack of opportunity. It simply takes time for exploitation methods to mature.

Furthermore, there may be a difference in terms of risk. The DNSChanger/Zlob Trojan does not presently exploit any software vulnerabilities, unless you could count bad passwords on SOHO routers. Its original victims willingly installed the Trojan, typically because they believed that it would decode pornographic videos. For multiple reasons, its victims might be embarrassed about their infection and unwilling to go very far in their response. If pressed, the operators of the Trojan might also argue that they have not committed any crime, as the installation was voluntary, although the cracking of SOHO router passwords sheds some doubt on the credibility of that claim. Nevertheless, a large-scale effort to exploit vulnerabilities in a critical part of the Internet's infrastructure is a great deal more brazen. Network operators with vast investigative resources might be willing to go very far in responding to such a threat, and that potential response changes the economic equation considerably.

Nevertheless, it is clear that there is money to be made poisoning DNS caches and that criminals know how to make that money. At the outset, this vulnerability represented a tremendous long-term risk to the Internet. The massive effort this summer to raise awareness and install patches has made the universe of vulnerable servers much smaller than it would otherwise be. Why put effort into developing a totally new attack technique when the one you are currently using works just fine and the new opportunity is dwindling fast? If the remaining population of vulnerable servers stays around for a long time, we may see a few attackers put their feet in the water. Things would be very different if these patches were being adopted more slowly and there was a larger pool of targets out there right now. So did all the media hype this summer save the Internet? Maybe so.

Conclusion

To put all of these issues into perspective, let's consider them together. Figure 7 plots each issue into one of four quadrants based on the opportunity they present to a criminal and the cost of realizing that opportunity. Only issues that make it to the top right resulted in widespread exploitation. The others did not present enough of a financial opportunity or they were too expensive to monetize.

If the security industry can learn to recognize vulnerabilities that fit into the top right quadrant of this graph, it can do a better job of determining when emergency patching is most needed in the face of immediate threats, when widespread exploitation of a vulnerability will take a long time to emerge, and when it is unlikely to ever emerge. This analysis is somewhat orthogonal to the technical analysis that currently takes place, and it is our view that it could result in more efficient use of time and resources.

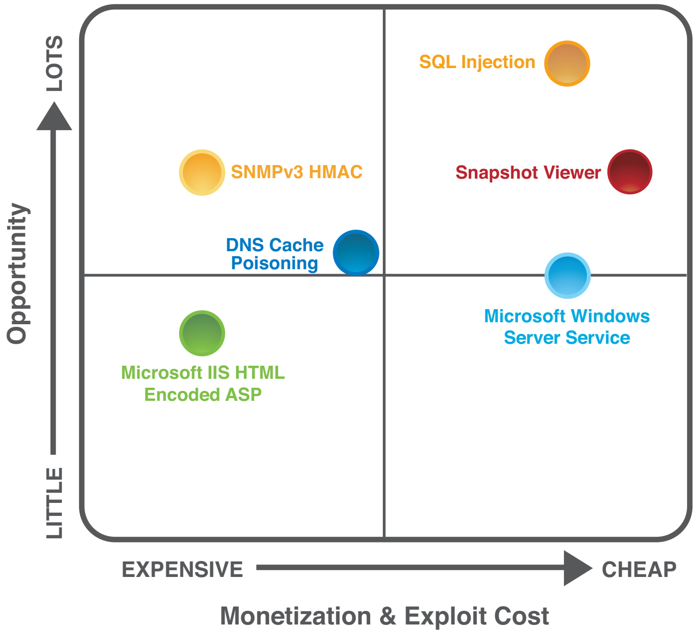


Figure 7: Exploitability Probability Quadrant

But, enough about what did not happen in 2008. The rest of this report focuses on what did happen last year and what might happen in 2009. As you read through the topics, it is helpful to keep this economic analysis in mind. Don't just consider the severity and ease of exploitation of a security issue, but the monetization challenges and economic opportunity that will determine whether or not computer criminals take advantage of that issue on a widespread basis.

Vulnerabilities

2008 Vulnerability Disclosure Count

X-Force analyzed and documented a record number of vulnerabilities in 2008. The 7,406 new vulnerabilities represent 19 percent of all vulnerabilities chronicled since the inception of the X-Force Database more than ten years ago.

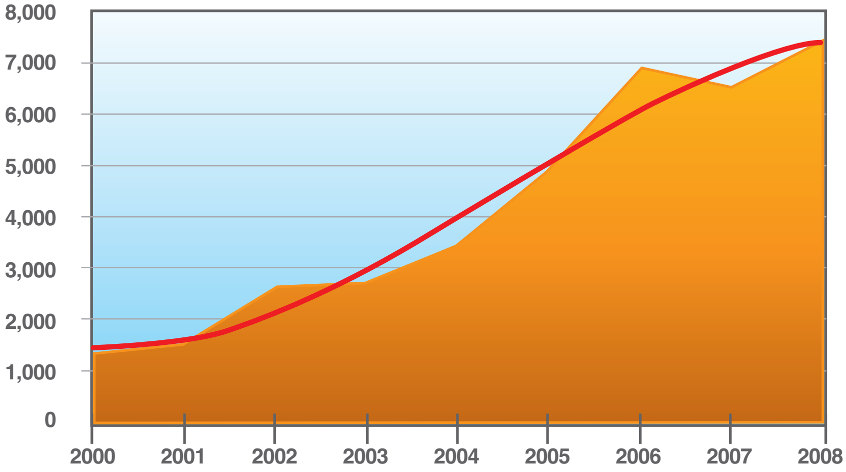


Figure 8: Vulnerability Disclosures, 2000 – 2008

To avoid any ambiguity regarding the characterization of vulnerabilities, the IBM Internet Security Systems (ISS) definition below is applied to this report.

Vulnerability – any computer-related vulnerability, exposure, or configuration setting that may result in a weakening or breakdown of the confidentiality, integrity, or accessibility of the computing system.

2008 saw the first year of over 7,000 total vulnerability disclosures (a 13.5 percent increase from 2007). From 2001 to 2006, the average annual vulnerability disclosure percentage growth was a robust 36.5 percent, largely due to the skyrocketing of Web application vulnerabilities, emergence of new Web technologies, and methods and tools of exploitation. From 2006 to 2008, the growth has tapered off to less than 2 percent average growth.

Although the introduction of new technologies or changes in vendor adoption of secure software practices might change this trend, for the moment at least, it appears as if vulnerability disclosures have reached a permanently high plateau.

Vulnerability Disclosure Timing

In addition to recording the highest year in vulnerability disclosures, X-Force also recorded a new record high for monthly disclosures, June 2008, in which 692 vulnerabilities were disclosed, replacing the previous record of 679 from May 2006. Although summer months are busy when it comes to vulnerability disclosures, the busiest week for disclosures typically happens around the holidays.

Year	Busiest Week for Vulnerability Disclosures
2000 – 2005	Week before Christmas
2006	Week before Thanksgiving
2007	Summer
2008	Week before Christmas

Table 1: Busiest Week for Vulnerability Disclosures

Tuesday remained the day of the week with the most new vulnerabilities observed, a trend that started in 2005. In 2008, X-Force chronicled 1,234 vulnerabilities on Mondays, followed by 1,548 on Tuesdays. The rest of the week saw a gradual decline in new vulnerability disclosures, while Saturday and Sunday continued to be well below the weekday average.

The jump in Tuesday vulnerabilities can be explained by the large number of vendor-released vulnerability advisories and patches on the second Tuesday of each month. Microsoft began the trend in Q3 2004 by regularly disclosing security bulletins on the second Tuesday of each month, and other large vendors began to follow suit for a variety of competitive or strategic reasons. Patch Tuesday, as it is commonly referred to in security circles, looks to keep Tuesday the busiest day of the week as long as the current large vendor disclosure paradigm holds true.

Vulnerability Disclosures by Severity

The X-Force uses multiple methodologies to classify the severity of vulnerabilities. However, starting with this annual report, only the Common Vulnerability Scoring System (CVSS) will be used to compare year over year changes in vulnerability severity.

CVSS is the industry standard for rating vulnerability severity and risk based on metrics (base and temporal) and formulas. Base metrics are comprised of characteristics that generally do not change over time. Base metrics include access vector, complexity, authentication, and the impact bias. Temporal metrics are made up of characteristics of a particular vulnerability that can and often do change over time, and include the exploitability, remediation level, and report confidence.

Vulnerabilities identified as Critical by CVSS metrics are vulnerabilities that are installed by default, network-routable, do not require authentication to access and will allow an attacker to gain system or root level access.

Table 2 represents the severity level associated with both the base and temporal CVSS scores.

CVSS ScoreLevel	Severity Level
10	Critical
7.0 – 9.9	High
4.0 – 6.9	Medium
0.0 – 3.9	Low

Table 2: CVSS Score and Corresponding Severity Level

For more information about CVSS, a complete explanation of CVSS and its metrics are on the First.org Web site at http://www.first.org/cvss/.

CVSS Base Scores

Critical and High vulnerability percentages remain largely unchanged from 2007, although vulnerabilities in 2008 saw an overall increase in Base score.

As Figure 9 indicates, only about 1 percent of all vulnerabilities scored in the Critical category in 2008, a slight decrease over 2007 where the percentage of critical vulnerabilities was 2 percent. While Critical vulnerabilities decreased slightly, the percentage of High vulnerabilities increased slightly, going from 36 percent in 2007 to 37.6 percent in 2008.

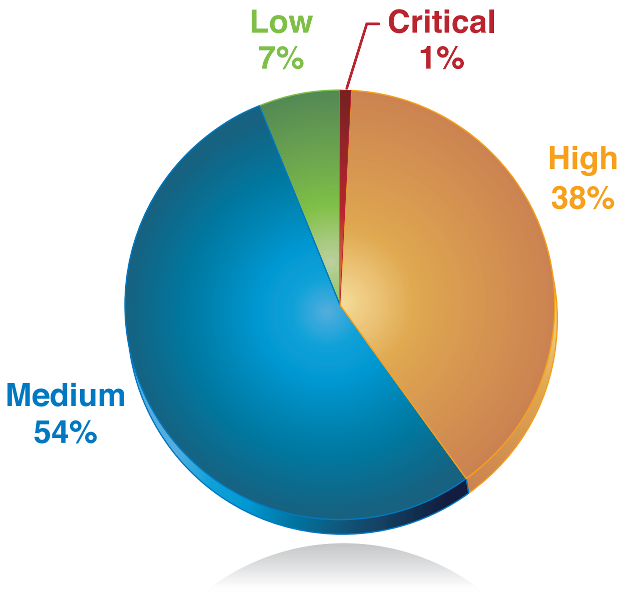


Figure 9: CVSS Base Scores, 2008

Medium and Low vulnerabilities, on the other hand, saw a significant shift in base score percentages, which accounted for the 2008 increase in base score severity (Figure 10). In 2007, 36.7 percent of vulnerabilities were classified as Medium, while in 2008, the percentage jumped to 54.0 percent. Low vulnerabilities correspondingly dropped from 25.4 percent in 2007 to 7.4 percent in 2008.

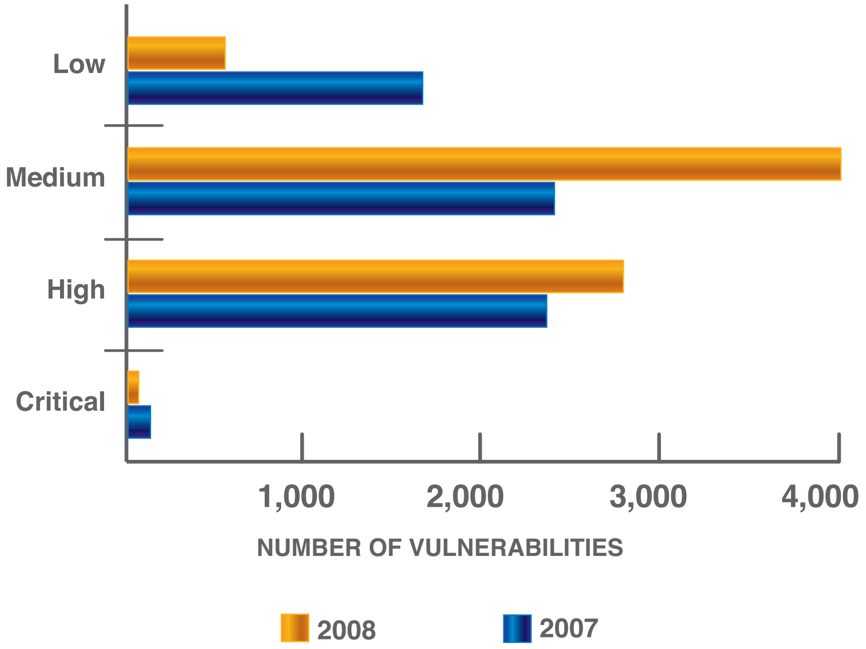


Figure 10: CVSS Base Scores, 2007 – 2008

CVSS Temporal Scores

Temporal metrics are made up of characteristics that apply to a particular vulnerability that can and often do change over time, and include the exploitability, remediation level, and report confidence.

Temporal scores, like base scores, also saw overall severity increase in 2008 (Figure 11). Vulnerabilities with a High temporal score more than tripled, jumping from 6.5 percent in 2007 to 21.6 percent in 2008. Medium score vulnerabilities stayed roughly the same, dropping from 53.1 percent in 2007 to 49.6 percent in 2008. Vulnerabilities with a low score dropped significantly, going from 40.5 percent in 2007 to 28.9 percent in 2008.

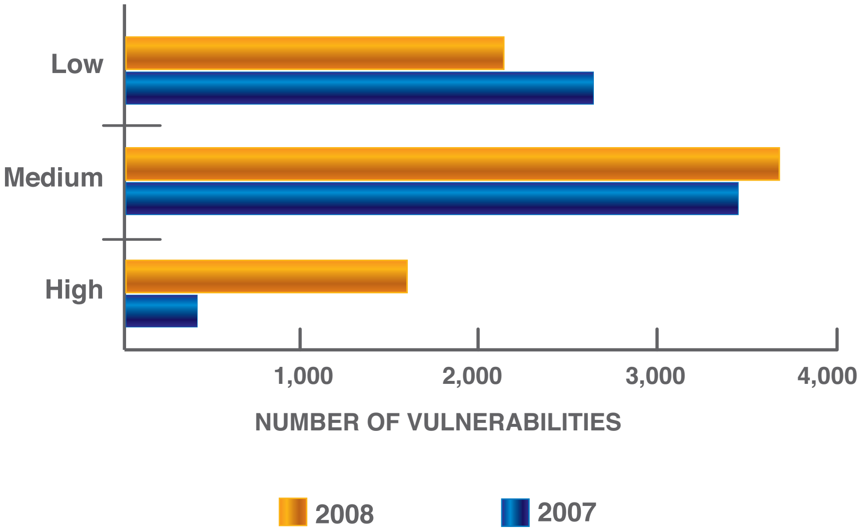


Figure 11: CVSS Temporal Scores, 2007 – 2008

Vendors with the Most Vulnerability Disclosures

Vulnerability disclosures for the top ten vendors in 2008 accounted for approximately 19.4 percent of all disclosed vulnerabilities, up less than one percentage point over 2007. Table 3 reveals who the top ten vendors are and their percentages of vulnerabilities in 2008.

These statistics do not balance vulnerability disclosures with market share, number of products, or the lines of code that each vendor produces. In general, mass-produced and highly distributed or accessible software is likely to have more vulnerability disclosures.

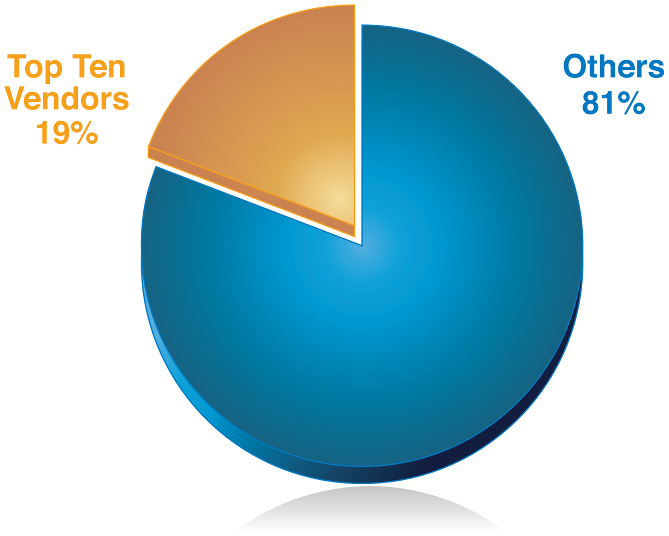


Figure 12: Percentage of Vulnerability Disclosures Attributed to Top Ten Vendors

New Vendors in the Top Vendor List

In 2008, the X-Force database team incorporated a new standard to classify vulnerabilities by vendor. This new standard is called CPE, or Common Platform Enumeration (more info at http://cpe.mitre.org/). This new methodology plus some changes in the vulnerability landscape brought some newcomers to our top ten list in the 2008 Mid-Year report:

- *Joomla!, an open-source content management system for Web sites*
- *WordPress, a blog publishing software*
- *Drupal, another open-source content management system for Web sites*

An obvious trend demonstrated by the appearance of these vendors on the top ten list is the increasing prevalence of Web-related vulnerabilities, described in detail in the Web Application Vulnerabilities section on page 31. Another commonality between these three vendors is that they are all written in PHP. If we look back over 2007 disclosures and apply the new CPE methodology to them, we would uncover another newcomer to the top five list, PHP itself, which would rank number four in the 2007 top five vendor list.

For the final 2008 tally, these newcomers have changed slightly. Joomla! And Drupal remain, but Linux and Wordpress dropped off the chart. Taking their spots are:

- *TYPO3, another open-source content management system for Websites*
- *Mozilla, most famously known for Mozilla Firefox, an open-source Web browser, but also a manufacture of other software products*

TYPO3 is even more similar to Joomla! and Drupal. All three are cross-platform, open source Web Content Management System (CMS) products written in PHP. Each of these products allows for simple Web publishing and typically interacts with open source back-end databases such as MySQL or PostgreSQL. Popular and modular products like these have code bases developed and shared by end users. We can expect the number of vulnerabilities to increase in this kind of category in correlation to each product's popularity and code base size.

Mozilla is also a new entrant when compared to the 2008 mid-year report. However, over 70% of Mozilla's 2008 vulnerability disclosures happened in the second half of this year.

Ranking	Vendor	Disclosures
1.	Microsoft	3.16%
2.	Apple	3.04%
3.	Sun	2.19%
4.	Joomla!	2.07%
5.	IBM	2.00%
6.	Oracle	1.65%
7.	Mozilla	1.43%
8.	Drupal	1.42%
9.	Cisco	1.23%
10.	TYPO3	1.23%

Table 3: Vendors with the Most Vulnerability Disclosures

Availability of Vulnerability Fixes and Patches

At the end of 2008, 53 percent of all vulnerabilities disclosed during the year had no vendor-supplied patches available to remedy the vulnerability. Vendors do not always go back to patch previous year's vulnerabilities. 46 percent of vulnerabilities from 2006 and 44 percent from 2007 were still left with no available patch at the end of 2008.

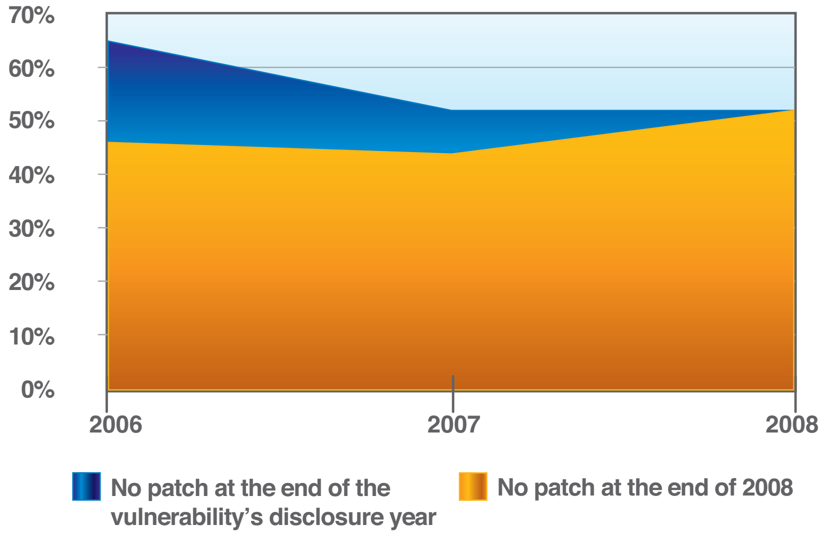


Figure 13: Percentage of Vulnerabilities with Vendor-Supplied Patches by Vulnerability Disclosure Year, 2006 – 2008

The top ten vendors with the most vulnerability disclosures did significantly better, with only 19 percent without patches, especially when compared to the remaining vendors that left 61 percent of their 2008 vulnerabilities without a patch.

These calculations take into account vendors that have publicly acknowledged a vulnerability and released a corresponding fix or patch. They do not take into account cases where a vendor silently fixes a vulnerability without an announcement, or a patch is released by a third-party vendor.

Remotely Exploitable Vulnerabilities

The most significant vulnerabilities are those that can be exploited remotely, because they do not require physical access to a vulnerable system. Remote vulnerabilities can be exploited over the network or Internet, while local vulnerabilities need direct system access.

2008 marks the third straight year where the percentage of remotely exploitable vulnerabilities has reached a record high. In 2008, they represented 90.2 percent of all vulnerabilities, up from 89.4 percent and 88.4 percent in 2007 and 2006 respectively.

A factor in the increase that has occurred over the past few years is the growing number of Web application vulnerabilities, which are typically remotely exploitable and an ever-growing percentage of the overall vulnerability count. Figure 14 shows the growth in remotely exploitable vulnerabilities year over year.

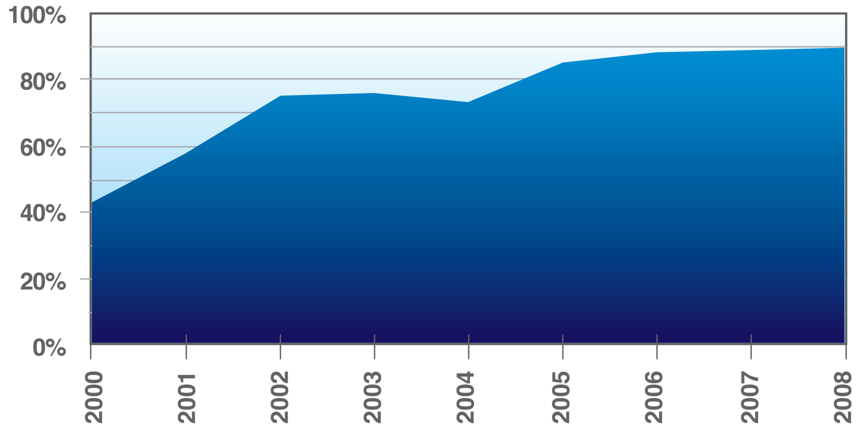


Figure 14: Percentage of Remotely Exploitable Vulnerabilities, 2000 – 2008

Consequences of Exploitation

X-Force categorizes vulnerabilities by the consequence of exploitation. This consequence is essentially the benefit that exploiting the vulnerability provides to the attacker. Table 4 describes each consequence.

Consequence	Definition
Bypass Security	Circumvent security restrictions such as a firewall or proxy, and IDS system or a virus scanner
Data Manipulation	Manipulate data used or stored by the host associated with the service or application
Denial of Service	Crash or disrupt a service or system to take down a network
File Manipulation	Create, delete, read, modify, or overwrite files
Gain Access	Obtain local and remote access. This also includes vulnerabilities by which an attacker can execute code or commands, because this usually allows the attacker to gain access to the system
Gain Privileges	Privileges can be gained on the local system only
Obtain Information	Obtain information such as file and path names, source code, passwords, or server configuration details
Other	Anything not covered by the other categories

Table 4: Definitions for Vulnerability Consequences

The most prevalent primary consequence of vulnerability exploitation continues to be Gain Access, although it is down slightly in comparison to previous years. Gaining access to a system provides an attacker complete control over the affected system, which would allow them to steal data, manipulate the system, or launch other attacks from that system. Most other attack vectors also remain similar to previous years, with the exception of Data Manipulation, which has practically doubled and is attributed to the rise in SQL injection Web application vulnerabilities, as described in Web Application Vulnerabilities on page 31.

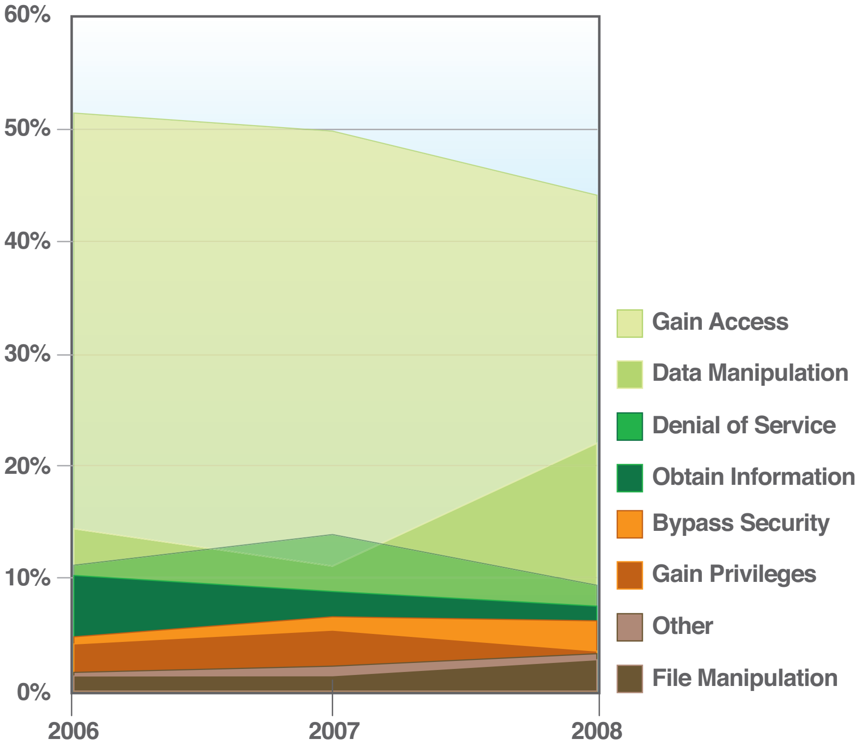


Figure 15: Vulnerability Consequences as a Percentage of Overall Disclosures, 2006 – 2008

Web Application Vulnerabilities

The most prevalent type of vulnerability affecting servers today is unquestionably vulnerabilities related to Web applications.

The number of vulnerabilities affecting Web applications has grown at a staggering rate. In 2008, vulnerabilities affecting Web server applications accounted for 54 percent of all vulnerability disclosures and were one of the primary factors in the overall growth of vulnerability disclosures during the year.

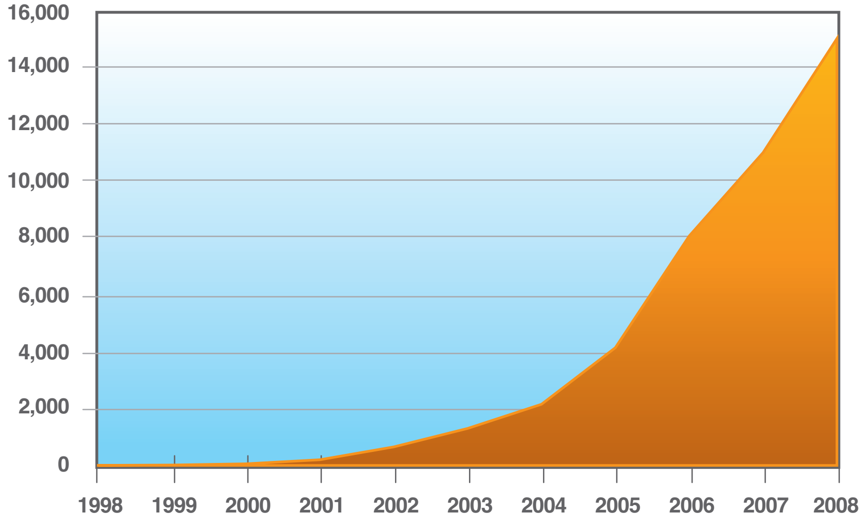


Figure 16: Cumulative Count of Web Application Vulnerabilities, 1998 – 2008

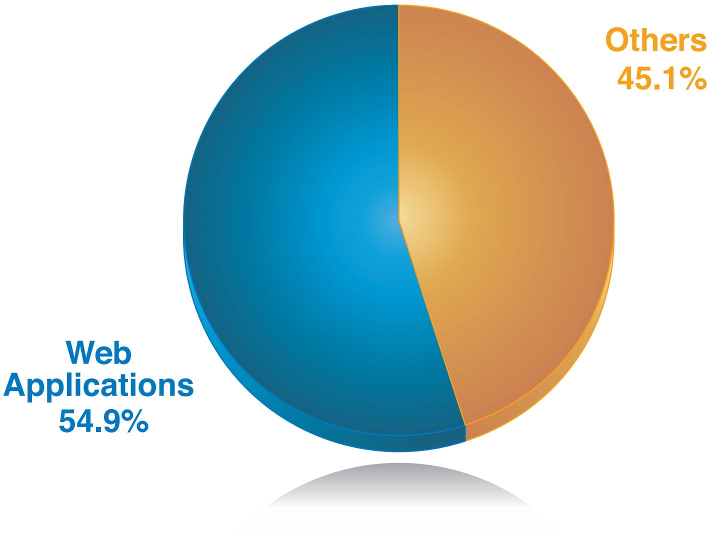


Figure 17: Percentage of Disclosures that are Web Application Vulnerabilities, 2008

Web Application Vulnerabilities by Attack Categories

The predominate types of vulnerabilities affecting Web applications are cross-site scripting (XSS), SQL injection, and file include vulnerabilities. In 2008, SQL injection replaced cross-site scripting as the predominant Web application vulnerability. In fact, the overall increase of 2008 Web application vulnerabilities can be attributed to a huge spike in SQL injection vulnerabilities, which was up a staggering 134 percent from 2007 (Figure 19).

Although cross-site scripting issues are also easy to discover, they are not as valuable to an attacker. They usually result in cookie theft, which provides the attacker with access to a victim's account on the vulnerable Website. SQL injection, on the other hand, is often used to redirect the visitors from the vulnerable Website to the attacker's Website where remote code execution exploits can be launched against the victim's browser. So, the financial profile for the average cross-site scripting vulnerability is different than for the average SQL injection vulnerability. The value of controlling a user's account on a particular Website depends on what that Website is used for. On the other hand, having complete control of the user's computer and potentially all of that user's accounts on every Website they visit is always valuable, no matter how important the initial, vulnerable Website was.

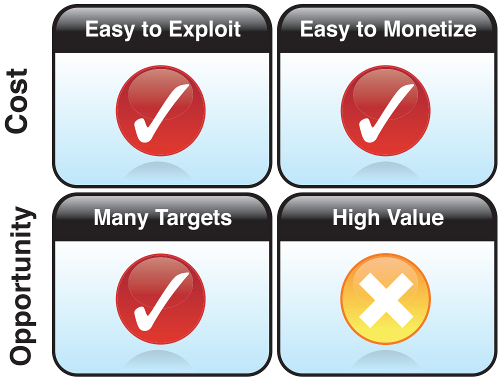


Figure 18: Exploitation Probability for Cross-Site Scripting

SQL injection vulnerabilities are plentiful and easily discovered. It also possible to use Web search engines such as Google to find sites running vulnerable applications, and there are many publicly available tools that can test for SQL injection, including some plug-ins for Firefox. It is not immediately clear whether SQL injection vulnerabilities increased because Web application vendors were releasing products with more vulnerabilities, or if there simply were more researchers testing for those vulnerabilities, although it is likely a combination of the two. What is clear is that major vendors took notice in 2008. For example, SQL injection attacks against Microsoft ASP and ASP.NET technologies prompted Microsoft to release a major security advisory on June 24 (Microsoft Security Advisory 954462).

Figure 19 shows how SQL injection and other major categories of Web application vulnerabilities have changed over the years, and Table 5 describes each category including the impact they can have on organizations and the customers they serve.

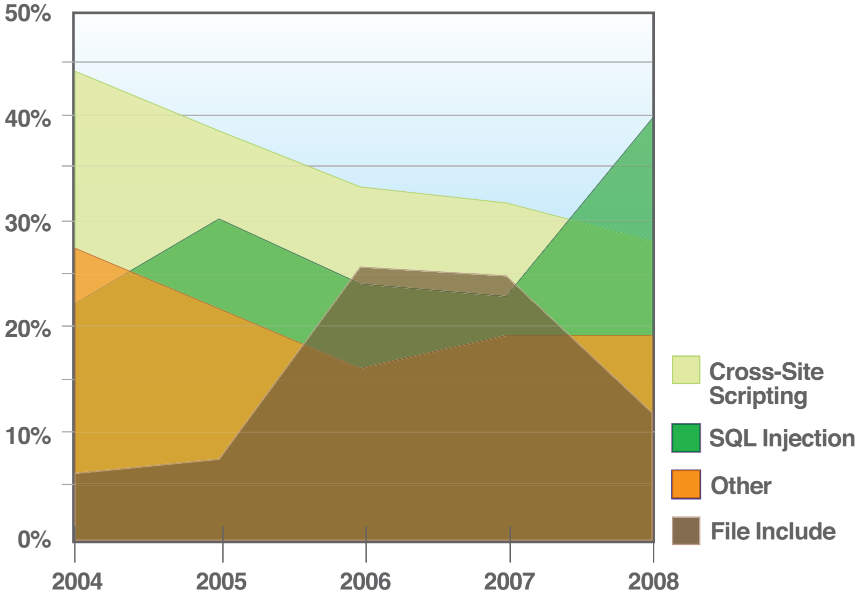


Figure 19: Web Application Vulnerabilities by Attack Technique, 2004 – 2008

Attack Technique	Description
Cross-site Scripting	Cross-site scripting vulnerabilities occur when Web applications do not properly validate user input from form fields, the syntax of URLs, etc. These vulnerabilities allow attackers to embed their own script into a page the user is visiting, 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 more content on the page that exploits other vulnerabilities. The attacker first has to create a specially-crafted Web link, and then entice the victim into clicking it (through spam, user forums, etc.) The user is more likely to be tricked clicking the link, because the domain name of the URL is a trusted or familiar company. The attack attempt may appear to the user to come from the trusted organization itself, and not the attacker that compromised the organization's vulnerability.
SQL Injection	SQL injection vulnerabilities are also related to improper validation of user input, and they occur when this input (from a form field, for example), is allowed to dynamically include SQL statements that are then executed by a database. Access to a back-end database may allow attackers to read, delete, and modify sensitive information, and in some cases execute arbitrary code. In addition to exposing confidential customer information (like credit card data), SQL injection vulnerabilities can also allow attackers to embed other attacks inside the database that can then be used against visitors to the Web site.
File Include	File include vulnerabilities (typically found in PHP applications) occur when the application retrieves code from a remote source to be executed in the local application. Oftentimes, the remote source is not validated for authenticity, which allows an attacker to use the Web application to remotely execute malicious code.
Other	This category includes some denial-of-service attacks and miscellaneous techniques that allow attackers to view or obtain unauthorized information, change files, directories, user information or other components of Web applications.

Table 5: Description of the Most Prevalent Categories of Web Application Vulnerabilities

Active Exploitation & Automated SQL Injection Attacks in 2008

In the past, most Web server compromises had been one-off, targeted exploitation attempts that steal information or manipulate an application in a way that is beneficial to the attacker. In the fist half of 2008, X-Force began tracking mass Web site exploitation using automated SQL injection attacks. Instead of leveraging SQL injection to steal data, this attack updated the application's back-end data to include iFrames to redirect visitors to malicious Web pages. These attacks targeted many well-known and trusted Web sites and were also integrated into the ASPROX exploit toolkit. Soon after, the number of attacks and sources of attacks began to explode as exemplified through the following data collected through IBM ISS Managed Security Services attack monitoring:

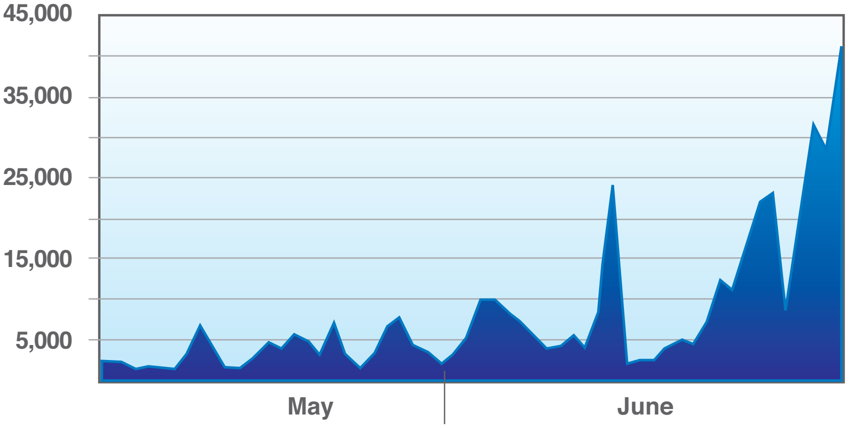


Figure 20: Initial SQL Injection Attacks Monitored by IBM ISS Managed Security Services, May – June 2008

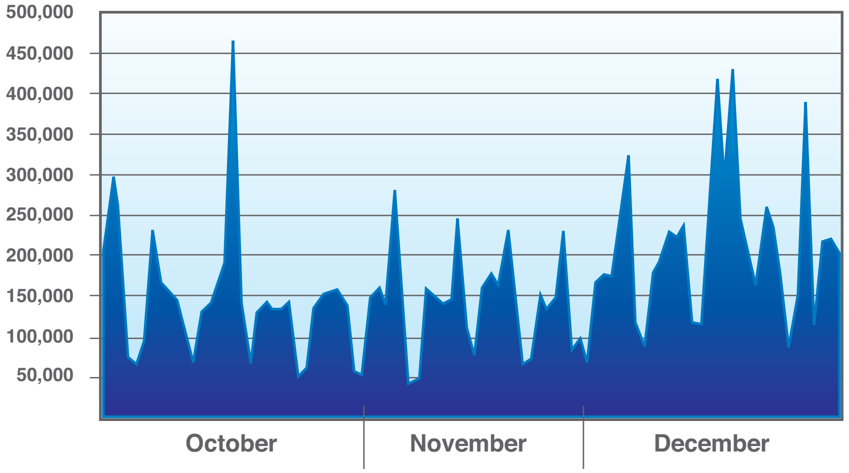


Figure 21: SQL Injection Attacks Monitored by IBM ISS Managed Security Services, Q4 2008

No Patch for You

An incredible number of vulnerabilities in Web applications have no vendor-supplied patch to fix the issue. Out of all the disclosures in 2008, 74 percent had no patch by the end of 2008. Again, this figure does not take into account custom-developed Web applications that may not have had any vulnerability testing and may never see a public vulnerability disclosure to notify the developer of a Web site about vulnerability issues and potential exploitation.

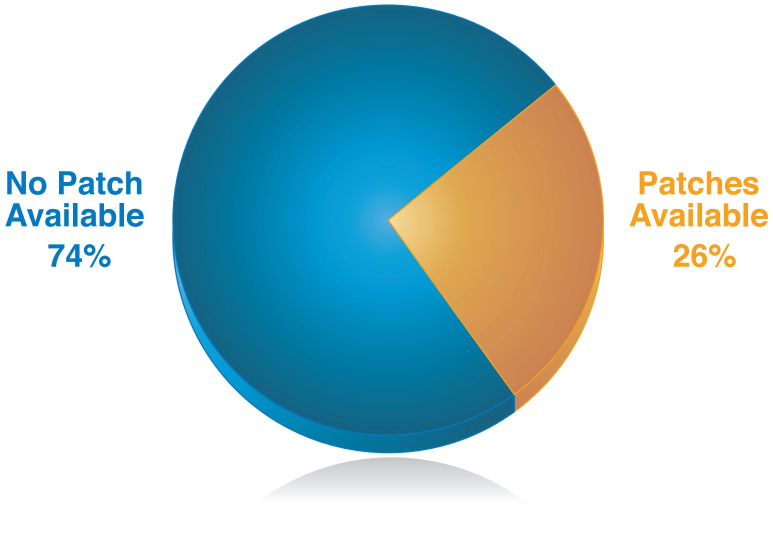


Figure 22: Percent of 2008 Web Application Vulnerabilities with No Vendor-Supplied Patch Available at the End of 2008

Good Websites Using Bad ActiveX Controls

One common practice that is evident in a detailed analysis of Web browser attacks is that many non-malicious Websites are continuing to propagate the use of known, vulnerable ActiveX controls. This practice has several downsides. First, from a customer and employee perspective, the user may be required to install the vulnerable ActiveX control. Although there are ways to redirect users to a fixed version of the control, the redirect will not work unless they are running an updated version of Internet Explorer or other ActiveX-enabled software that tracks and blocks these known vulnerable controls. If they do load the vulnerable control, and then browse to a malicious Website that uses an exploit for that control, they will be exploited without the normal prompt asking if they would like to install something new. If the control is already there, then they simply have no chance.

From a protection perspective, the use of these known vulnerable controls on non-malicious Websites creates a lot of "noise" that can mask real, malicious activity.

At the end of 2008, some of the bad ActiveX controls found on good Websites were:

ActiveX Control	Description
Aurigma ImageUploader 4.1	The Aurigma ImageUploader 4.1 ActiveX control (ImageUploader4.ocx) is vulnerable to a stack-based buffer overflow. References: CVE-2008-0659 ClassID: F1F51698-7B63-4394-8743-1F4CF1853DE1
BusinessObjects RptViewerAX	The BusinessObjects RptViewerAX ActiveX control (RptViewerAX.dll) is vulnerable to a stack-based buffer overflow. References: CVE-2007-6254: ClassID: B20D9D6A-0DEC-4D76-9BEF-175896006B4A
Macrovision InstallShield InstallScript One-Click Install	The InstallShield InstallScript One-Click Install ActiveX Control could allow a remote attacker to execute code on the system. References: CVE-2007-5661 ClassID: 53D40FAA-4E21-459F-AA87-E4D97FC3245A
Macrovision InstallShield Update Service Web Agent	The Macrovision ActiveX control (isusweb.dll), which is included in the InstallShield Update Service is vulnerable to a buffer overflow, caused by improper bounds checking by the DownloadAndExecute() function. References: CVE-2007-0321 ClassID: E9880553-B8A7-4960-A668-95C68BED571E
Microsoft MDAC RDS Dataspace	Microsoft Data Access Components (MDAC) could allow a remote attacker to execute arbitrary code, caused by a vulnerability in the RDS.Dataspace ActiveX object that is part of the Active X Data Objects (ADO) and distributed in MDAC. References: MS06-014/CVE-2006-0003 ClassID: AB9BCEDD-EC7E-47E1-9322-D4A210617116
Microsoft WebViewFolderIcon	Microsoft Internet Explorer could allow a remote attacker to execute arbitrary code on the system, caused by an integer underflow vulnerability in the Microsoft Windows Shell that can be exploited when processing a malformed WebViewFolderIcon ActiveX object with an invalid argument to the “setSlice” method. References: MS06-057/CVE-2006-3730 ClassID: 844F4806-E8A8-11D2-9652-00C04FC30871

Table 6: Known Vulnerable ActiveX Controls Used by Non-Malicious Websites

Most Vulnerable Operating Systems

X-Force tracks vulnerabilities by platform and has produced metrics this year to show the operating systems with the most disclosed vulnerabilities. The following chart shows the operating systems with the most vulnerabilities documented in 2008. The top ten operating systems account for nearly 75% of all vulnerability disclosures affecting operating systems.

Operating System	Percentage
Apple Mac OS X Server	14.3%
Apple Mac OS X	14.3%
Linux Kernel	10.9%
Sun Solaris	7.3%
Microsoft Windows XP	5.5%
Microsoft Windows 2003 Server	5.2%
Microsoft Windows Vista	5.1%
Microsoft Windows 2000	4.8%
Microsoft Windows 2008	4.1%
IBM AIX	3.7%
Others	24.9%

Table 7: Operating Systems with the Most Vulnerability Disclosures, 2008

Several operating systems have remained in the top five list over the past three years:

- *Apple Mac OS X*
- *Apple Mac OS X Server*
- *Linux Kernel*
- *Microsoft Windows XP (with one exception in 2007)*

Browser and Other Client-Side Vulnerabilities and Exploits

Vulnerabilities affecting personal computers are the second-largest category of vulnerability disclosures after Web application vulnerabilities and represent around one fifth of all vulnerability disclosures.

Client-side vulnerabilities: Vulnerabilities affecting the operating system or applications running on personal computers. In addition to the core operating system, vulnerable components could include e-mail clients, Web browsers, document viewers, and multimedia applications.

Client-Side Vulnerabilities – Browsers Are Getting Better

The overall number of vulnerability disclosures affecting personal computers went down in 2008, which can be attributed to a few key categories. The two biggest contributors to the decline are described in the following table.

Category	Overall Decline	Change in Critical and High Vulnerabilities
Browsers & browser plug-ins	10%	Held constant (about 300 disclosures in both 2007 and 2008)
VOIP clients	49%	Increased – nearly doubling the number disclosed in 2007

Table 8: Key Vulnerability Categories Related to the Overall Decline in Client-Side Vulnerability Disclosures in 2008

Even though the overall numbers were down, several categories of vulnerabilities showed significant increases. The most marked increase was related to Java, although it is important to note that Java vulnerabilities only account for around 4 percent of all client-side vulnerability disclosures.

- *Document readers and editors, up by 162 percent. These applications also had many more critical and high disclosures, which increased by 168 percent.*
- *Multimedia applications, up by 127 percent.*

Category	Overall Increase	Change in Critical and High Vulnerabilities
Java	264%	Held constant
Document Readers and Editors	162%	Increased – 168% over 2007
Multimedia	127%	Decreased – About half the number reported in 2007

Table 9: Client-Side Vulnerability Categories That Showed Significant Increases in 2008

Critical and High Vulnerability Disclosures in Prevalent Applications

As described in Exploitation Economics: What Didn't Happen in 2008 and Why on page 5, two factors that can affect the probability of mass exploitation include the benefit derived from exploiting the target (critical and high vulnerabilities) and the prevalence of targets to exploit. Certain categories of vulnerabilities affecting clients are arguably more pervasive than others. For example, although a significant percentage of vulnerabilities are related to VOIP software, this category of software is not nearly as pervasive as operating systems, browsers, multimedia applications, etc.

Figure 23 shows the changes in critical and high vulnerability disclosures for these types of applications. Although declining in number from 2007, browser-related vulnerabilities are still overwhelming the largest percentage of critical and high vulnerabilities affecting personal computers in 2008 (52 percent of all criticals and highs). At 6 percent, multimedia applications still represent a significant portion of criticals and highs, although they are down from 10 percent in 2007. Critical and high operating system vulnerabilities are still in decline. Probably the most interesting change categorically, is that of Document Readers and Editors. This category contains vulnerabilities disclosed in prevalent applications such as Microsoft Office and Adobe Acrobat among others. These applications represent 13 percent of all critical and high client-side disclosures in 2008 as compared to only 7 percent in 2007. This change is reflected in public exploitation X-Force has monitored throughout the year for these types of vulnerabilities. See Exploitation Targets: From the OS to the Browser and Beyond on page 47 for more details.

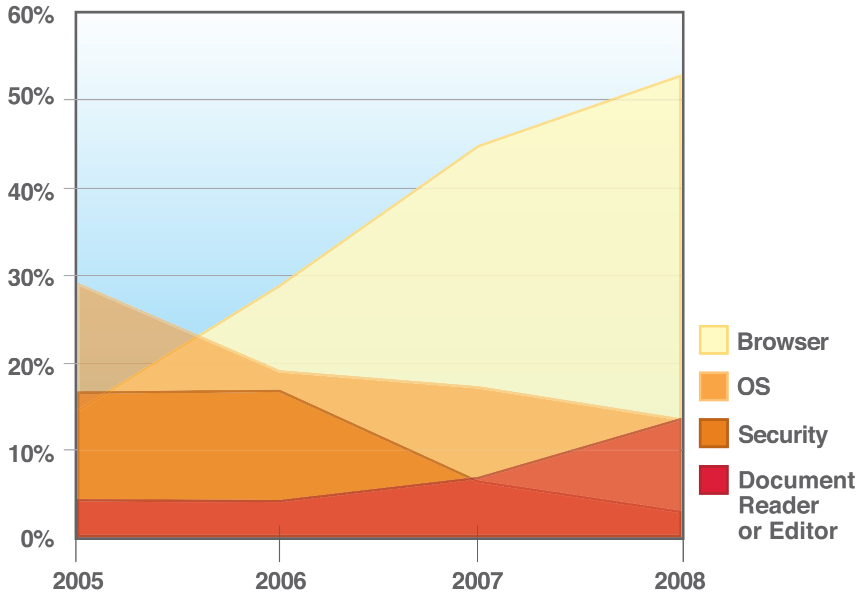


Figure 23: Critical and High Vulnerability Disclosures Affecting Client-Side Applications by Application Category, 2005 – 2008

Browser and Plug-in Vulnerabilities – ActiveX Disclosures Declining

The largest category of client-side vulnerabilities is the browser category. This category includes not only the browsers themselves but also the myriad plug-ins that can be installed on them. The most affected component out of all the browsers and types of plug-ins is the ever-pervasive ActiveX control, which represented 46 percent of all browser-related disclosures in 2008 and 66 percent of all critical and high browser-related vulnerabilities as shown in Figure 24. Even so, 2008 may be the pivotal year for ActiveX controls. In sheer number, these disclosures declined for the first time ever in 2008, which was the predominant factor behind the overall decline in browser-related disclosures.

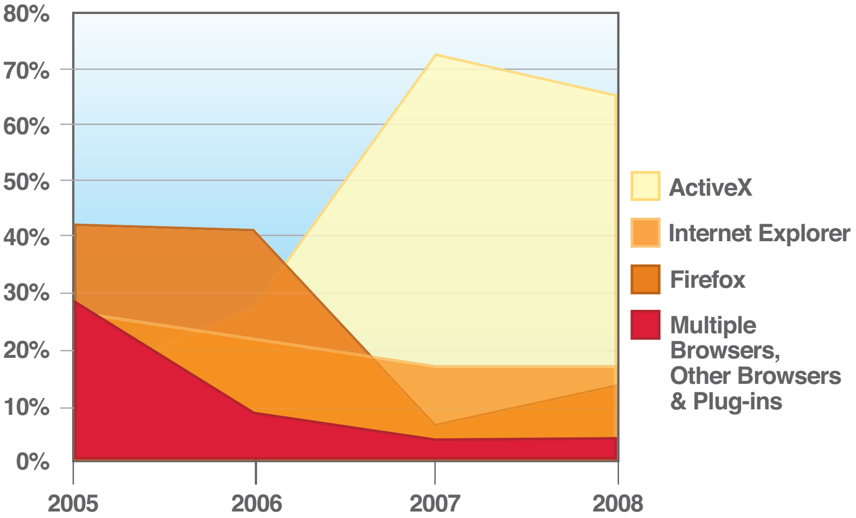


Figure 24: Critical and High Vulnerability Disclosures Affecting Browser-Related Software, 2005 – 2008

Unfortunately, the decline in ActiveX disclosures does not appear to be making an impact on exploitation. As with other browser-related vulnerabilities, attackers rely upon users who do not keep their browsers currently patched. Although Microsoft has made great strides in preventing ActiveX exploitation through changes to Microsoft Internet Explorer, exploitation remains an issue along with the continued usage of known vulnerable ActiveX controls from non-malicious Websites (see Good Websites Using Bad ActiveX Controls on page 38).

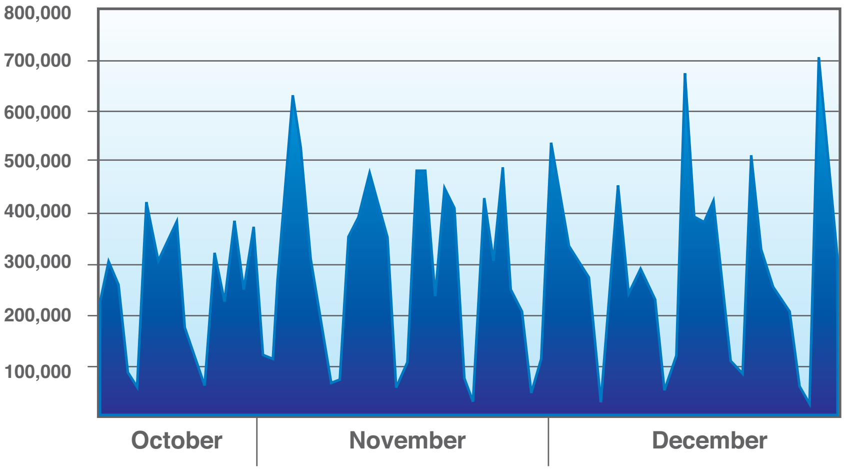


Figure 25: Vulnerable ActiveX Control Usage and Exploitation

Availability of 0-Day Exploit Code

The availability of public exploit code, either proof-of-concept or fully-functioning, is a key indicator that a vulnerability will suffer active exploitation. The X-Force definition of "public exploit" follows the standard CVSS terminology.

Public exploit: Any proof-of-concept demonstrative code, partially or fully functional, or malicious mobile agent, such as malware, that is publicly available.

Some researchers and research organizations will publish either proof-of-concept (PoC) code or enough details about the vulnerability so that another individual can quickly put together and publish a PoC. The public availability of proof-of-concept code increases the likelihood that the vulnerability will face live exploitation either through targeted attempts or through a mass distribution method, like in an exploit toolkit. Common outlets for these public exploits are testing tools like Metasploit and Canvas.

In prior years, it could take weeks or months to produce proof-of-concept exploits for vulnerability disclosures, but the number of days between public disclosure and public exploit availability has shrunk significantly. In 2008, 89 percent of these public exploits were released on the same day or before the official vulnerability disclosure. Browser-related exploits, in particular, are increasingly prone to same day exploit publication. In the first half of 2008, 94 percent of all browser-related public exploit code was published within 24 hours of official vulnerability disclosure, up from 79 percent in 2007. However, the remainder of 2008 showed some improvement in this area. By the end of 2008, only 89 percent of all browser-related public exploit code was published within 24 hours.

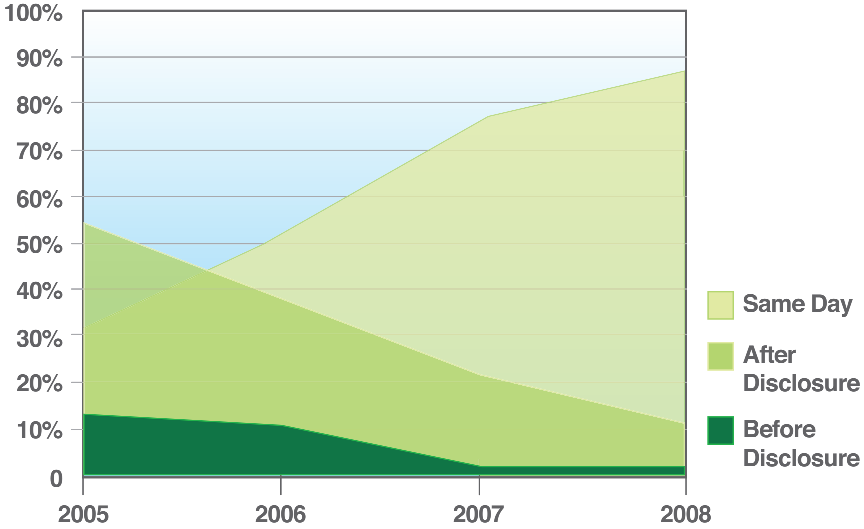


Figure 26: Rise in 0-day Exploits

Exploitation Targets: From the OS to the Browser and Beyond

Web Browser Exploitation Trends

X-Force continues to track growth in Web browser exploitation through its Whiro crawlers, which combined independent analysis with IBM ISS Managed Security Services operational alerting data. X-Force has developed specialized technology to identify exploits used even in the most obfuscated cases including where toolkits attempt multiple exploits.

During 2008, it became clear that lone Web browser exploits in the wild were dying out and being replaced by the organized use of Web exploit toolkits. These toolkits can deliver all of the exploits at once to Web site visitors, or the toolkit can select specific exploits based on data, such as:

- *Browser cookie set by the toolkit*
- *Browser agent used by the victim*
- *Geographic location derived from the victim's IP address*
- *Referrer URL (the URL that directed the victim to the Web site)*

In many instances, these toolkits provide easy-to-use management interfaces. Deployments of exploit toolkits are in some cases financially supported by multiple attackers who are credited by an id number associated in their attack URLs, which is interesting because it allows attackers to get a piece of the action with a smaller initial investment. Nevertheless, it is not known how many toolkit installations are actually purchased versus leased or pirated.

Most Popular Exploits

Rank	2008 (Full Year)	2008 H2 (Second Half)
1.	Microsoft MDAC RDS Dataspace ActiveX (CVE-2006-0003)	Microsoft MDAC RDS Dataspace ActiveX (CVE-2006-0003)
2.	RealPlayer IERPCtl ActiveX (CVE-2007-5601)	Microsoft WebViewFolderIcon ActiveX (CVE-2006-3730)
3.	Apple QuickTime RSTP URL (CVE-2007-0015)	Internet Explorer “createControlRange” DHTML (CVE-2005-0055)
4.	Microsoft WebViewFolderIcon ActiveX (CVE-2006-3730)	RealPlayer IERPCtl ActiveX (CVE-2007-5601)
5.	Internet Explorer “createControlRange” DHTML (CVE-2005-0055)	Apple QuickTime RSTP URL (CVE-2007-0015)

Table 10: Most Popular Web Browser Exploits, 2008

Compared with our mid-year report, there are still four from the last top five most popular Web browser exploits in both the second-half of the year as well as full-year results. This sort of trend has been observed over the past couple of years and in X-Force’s opinion, it is mostly a function of convenience with off-the-shelf toolkits and piracy. During 2008, the Neosploit kit team announced they were shutting down; however, it was later discovered by X-Force and others that updated copies of Neosploit are being used in the wild. Simply put, Neosploit was updated with several new exploits after the supposed shutdown.

Most Popular Exploit Toolkits (2H 2008)

Rank	2008 (Full Year)	2008 H2 (Second Half)
1.	mPack (and variants)	CuteQQ
2.	CuteQQ	AdM
3.	AdM	mPack (and variants)
4.	FirePack	Neosploit
5.	Neosploit	Tornado (and variants)

Table 11: Most Popular Exploit Toolkits, 2008

While many people believe that Web browser exploit toolkits are primarily distinct, this is not entirely true. In our mid-year report, we started the discussion of exploit toolkit popularity in terms that included variants. To maintain perspective, we may report a toolkit as unique, as a variant, or as both unique and as a variant. For example, the CuteQQ kit which is the most popular for the 2nd half of 2008 is related to the FirePack kit that dropped out of the top five list. The CuteQQ kit is based on another kit called SmartPack which, in turn, borrowed elements from FirePack.

While the Random.JS mPack derivative outbreak earlier in the year was responsible for a massive spike in mPack popularity at the time, the current state of mPack utilization is significantly lower. Nevertheless, mPack variants have claimed the top spot on our list as the most popular exploit toolkit over the full year.

Another interesting change since our mid-year report is that the second most popular kit listed in our mid-year report – previously unknown in name – has been absorbed by the CuteQQ kit family.

Obfuscation

During the second half of 2008, X-Force observed a reduction in obfuscation and specifically a reduction in the use of multiple layers of obfuscation. Obfuscation techniques typically have been both basic, such as string concatenation, as well as complex decoder stubs which themselves can be layered through the self-decoding process. In the recent past, X-Force identified what appeared to be an emerging trend of multiple self-decoding layers. By the end of 2008, pages with malicious script featuring self-decoding typically had no more than one of these layers and also predominately used basic string concatenation. We attribute the changes in code obfuscation to the shifts in the most popular exploit toolkits. Moving forward, it is hard to predict whether a reduction in obfuscation will continue as a new trend or whether obfuscation will intensify, again.

In the mid-year report, X-Force conveyed that the use of Visual Basic Script or VBScript with Web browser exploitation was three percent. Visual Basic Script is an older language native to the Internet Explorer browser. Other browsers such as Firefox, Opera, Chrome and Safari do not support this script language although they are targeted by attackers far less frequently due to market share. During the second half of 2008, VBScript utilization towards exploitation of IE increased on a per-site basis by 562%. Thus, while VBScript is still utilized by a small number overall, its increase indicates a potential trend. One possible explanation is that most detection solutions only support JavaScript analysis and therefore it is a form of obfuscation.

PDF Exploitation and Obfuscation

During 2008, there have been two significant PDF exploits deployed in the wild (CVE-2007-5659 and CVE-2008-2992). While individually not numerous enough to pierce our "Top 5", their integration into exploit toolkits occurred and is meaningful in terms of obfuscation. The vulnerabilities were in the object model created by Acrobat on top of a JavaScript engine and are subsequently exploited in this way. The exploit JavaScript took on the same characteristic obfuscation seen in exploit toolkits with decoder stubs, but then attackers discovered that they could use the DRM mechanism with a blank document password to encrypt the document with 40-bit or 128-bit RC4 keys. The significance is that decrypting the document even with a default key can be expensive on-the-wire and even now there may still be host-based security software that does not bother. Net, it was an interesting year for PDF exploit obfuscation and many, if not most, tricks to obfuscate attacks have been exposed.

Overall Client-Side Attack Activity

In addition to the Whiro project, X-Force monitors overall exploitation trends through several other sources:

- *ISS Managed Security Services, responsible for monitoring exploits related not only to endpoints, but also servers (including Web servers) and general network infrastructure. MSS monitors events covering:*
  - *7 Security Operation Centers*
  - *133 countries*
  - *15k+ devices*
  - *2200+ customers*
  - *400 million events per day*
  - *150 million intrusion attempts per day*

- *Our "C-Force," the researchers that support the IBM ISS Cobion Web-crawling products and technologies and are the main contributors to the spam, phishing, and Web content distribution sections of this report.*

Exploits from Malicious Websites

Our Content Filtering (Cobion) team works with our Managed Security Services to track and document malicious Websites. The number of malicious URLs hosting exploits in Q4 alone was 50 percent more than the number seen over the entire year of 2007. This trend is partially due to a technique used by some attackers to set up the same Website using many different URL names.

In 2007, malicious Websites hosting client exploits primarily focused on exploiting Web browsers or their plug-ins. Less than 1% of these Websites included attacks related to documents or multimedia applications. In 2008, multimedia exploits and document-related exploits also took a much stronger presence.

Analyzing the data by affected component shows a more telling story as shown Figure 27. Although most exploitation focuses on Microsoft-enabled technology (ActiveX and Internet Explorer), the rise in multimedia and document exploitation is attributed to Adobe software.

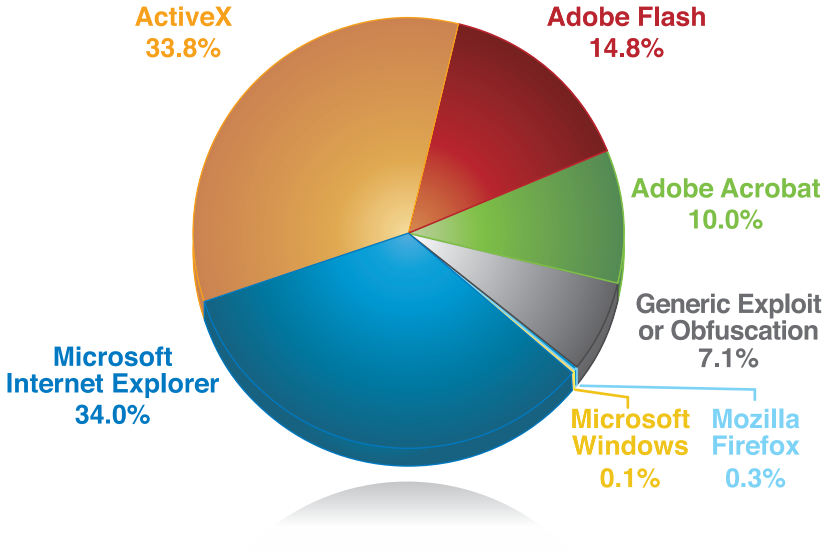


Figure 27: Malicious Website Exploits by Affected Application, ISS Cobion Crawler, 2008 Q4

Countries Hosting the Most Malicious Websites

Additionally, our data shows that the hosting source of malicious Websites has shifted this year. In the past, the US was the primary host of malicious Websites. In 2008, China took over as the country hosting the most malicious Websites.

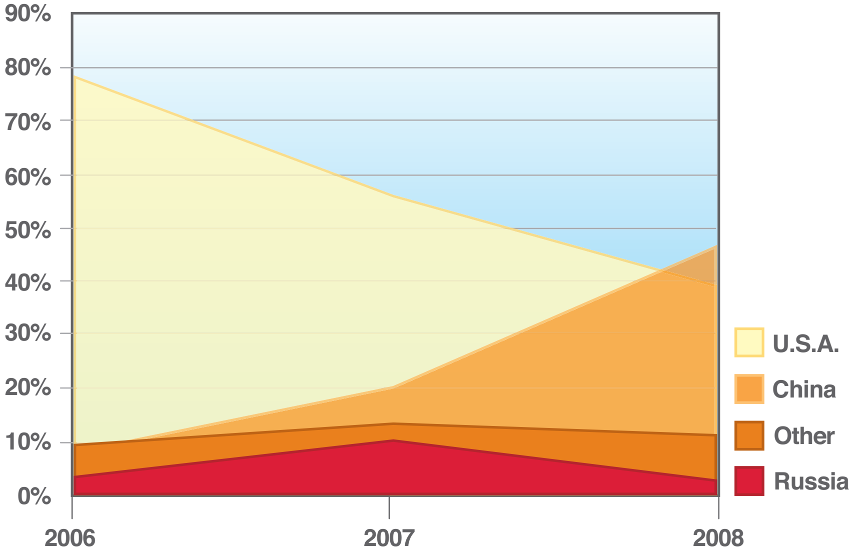


Figure 28: Malicious URLs by Hosting Country, ISS Cobion Crawler, 2006 – 2008

Spam

The IBM ISS premier content filtering services provide a world-encompassing view of spam and phishing attacks. With millions of e-mail addresses being actively monitored, X-Force 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 (every spam is broken into several logical parts [sentences, paragraphs, etc.], and a unique 128-bit signature is computed for each part) and millions of spam URLs. Each day there are one million new, updated or deleted signatures for the spam filter database.

The topics of this section are:

- *Changes in spam volume including the McColo takedown and how it changed the international distribution of spam*
- *New trends towards simpler spam*
- *Most popular domains used in spam*
- *Most popular Top Level Domains (TLDs) used in spam and why the top domains are so popular*
- *Lifespan of Spam URLs*
- *Spam's country*[1] *of origin trends, including spam Web pages (URLs)*
- *Changes in the average byte size of spam*
- *Most popular subject lines of spam*

[1] *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.*

Spam Volume

This year's spam volume has not evolved and expanded as in years past. Instead of steady increase, spam has flattened out near the middle of the year with a significant drop in November due to the McColo takedown. After increasing by about 50% from April to June, volume fell back to April levels by August, and then took a significant drop (75 percent) in November. As of December, volume had rebounded to 70 percent of the original level.

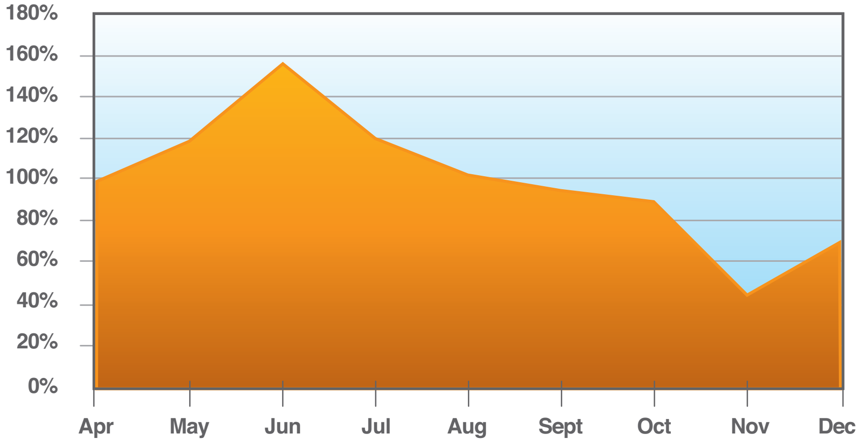


Figure 29: Changes in Spam Volume Since April, 2008

More Trends Towards Simpler Spam

In the past few years there has been a rise, and now a decline, in what X-Force considers "complex" spam types. The predominant type of complex spam was originally image-based spam, but there are many types of spam that fall into this "complex" category:

- *Image-based spam (including complex images with random pixels, random borders, or text on wavy lines)*
- *Animated GIF spam*
- *PDF spam*
- *Spam messages containing much random text, for example, from news sites or poems*
- *Spam messages containing complicated HTML frameworks that intersperse random characters between the actual spam text*

URL Spam

At the end of 2007, these complex types of spam began to decline and have continued to do so in 2008. So, what have the spammers used to replace these types of spam? Figure 30, which shows a rise in URL spam (spam e-mail that contains little more than a link to a Web site that delivers the spam message to the victim) and a converse decline in Image-based spam may provide the answer.

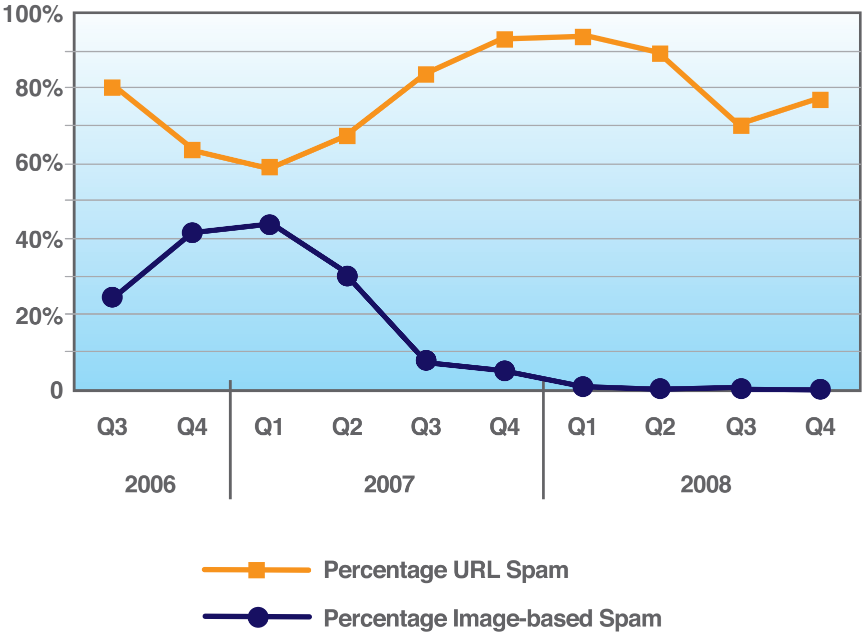


Figure 30: Percentage of Image-based Spam and URL Spam

The Rise and Fall of Plain-Text Spam

The percentage of simple, plain-text spam, spam that contains (typically) short, plain-text content and no HTML or attachments, grew primarily in parallel to the percentage of URL spam over the last two and a half years. However, at the end of 2008, plain-text spam started decreasing and, at the same time, URL spam increased.

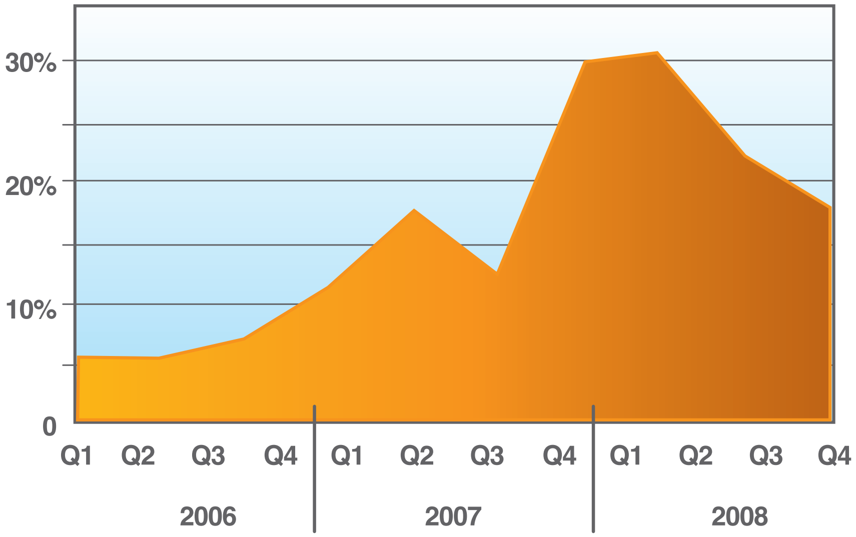


Figure 31: Changes in the Percentage of Simple, Plain-Text Spam

It is clear that spammers have started to abandon plain-text spam in favor of HTML spam, possibly because this plain-text spam has becoming increasingly suspicious, and therefore, less effective. All contemporary email clients support HTML emails, and most legitimate marketing and newsletter e-mail services use the more visually stimulating HTML email instead of plain text. So, perhaps using HTML for spam messages creates more legitimate-looking emails, which are most likely more effective.

The McColo shutdown also had a significant effect on the types of spam in circulation. For more details on the changes in spam during the shutdown, see The McColo Takedown on page 72.

Common Domains in URL Spam

Since URL spam is increasing, it is worthwhile to take a closer look at the most frequently used domain names in URL spam. The following tables show the top 10 domains per month throughout 2008, with a few key domains highlighted.

Rank	January 2008	February 2008	March 2008	April 2008	May 2008	June 2008
1.	googlepages.com	blogspot.com	blogspot.com	crazeben.com	doubleclick.net	dogpile.com
2.	sarahkverok.com	81.222.138.69	powref.com	manninst.com	livefilestore.com	kewww.com.cn
3.	magnarx.com	goldsmallman.com	nuelig.com	hyuaien.com	maddris.com	ynnsuue.com
4.	nesoeteaok.com	fastmansilver.com	gelsedde.com	pobueitah.com	nubteku.com	wpoellk.com
5.	lifefreeart.com	dotoneauto.com	mewlegos.com	congratym.com	moieiaus.com	movecontinent.com
6.	sgmykrtrewt.com	dedeiooss.com	findmilk.com	timeminute.com	coridez.net	moptesoft.com
7.	qualiveok.com	geocities.com	marketthen.com	camethank.com	zimpleq.com	varygas.com
8.	nightboylost.com	hotripefruit.com	seatbar.com	wroteleast.com	misllie.com	earexcept.com
9.	northmanestimate.com	topstopcool.com	believeagree.com	writecotton.com	pogieamdo.com	fullrow.com
10.	geocities.com	fastpetsilver.com	somelisten.com	saveany.com	poskeij.com	colonytop.com

Table 12: Most Common Domains in URL Spam, 2008 H1

Rank	July 2008	August 2008	September 2008	October 2008	November 2008	December 2008
1.	livefilestore.com	cnn.net	livefilestore.com	livefilestore.com	live.com	gucci.com
2.	smellshort.com	cnn.com	imageshack.us	live.com	tubdyqwenqe.com	notdune.com
3.	elementdepend.com	msn.com	beroyal.info	el1te-russ1an-g1rls.com	eurocasinokd.com	hereidea.com
4.	opera.com	msnbc.com	forformisskasino.com	myrusfriend.net	stop-fl0p.net	live.com
5.	grayany.com	imageshack.us	totalwrite.com	yellowpages.com	bbc.co.uk	heatdark.com
6.	creasehappiness.com	reoisk.com	cazinoyoumeyou.com	livechatfreex.com	hop-m0p.com	namenot.com
7.	msn.com	google.com	casinonewtrip.com	googlegroups.com	t1p-top.com	idolreplicas.com
8.	boceph.com	soieuu.com	csinomonster.com	cazinosostermor.com	eurocasinokg.com	davavkos.com
9.	alizedup.com	royalfirsteuro.info	beroyal.mobi	777-models-777.com	n1cewomen7.com	vutovlaf.com
10.	augsid.com	royalfirsteuro.mobi	beroyal.org	cazinomonste.com	sexymodels123.net	conemain.com

Table 13: Most Common Domains in URL Spam, 2008 H2

Although the majority of URL spam is hosted on domains that were obviously registered for spam purposes, the amount of URL spam using well-known and trusted domain names has significantly increased. In the first half of the year, these well-known domains made our monthly top ten list only 8 times. In the second half of the year, this count more than doubled with 19 spots filled with well-known names from July through December. In addition to new names appearing on the charts, a new trend of using news Web site domains has emerged, with a huge peak in the month of August.

Some of the well-know Websites are:

- *blogspot.com (blog publishing)*
- *doubleclick.net (develops and provides Internet ad serving services)*
- *google.com (Major Internet search engine)*
- *googlegroups.com (free service from Google where groups of people have discussions about common interests)*
- *googlepages.com (Google's Web site creation and hosting service)*
- *gucci.com (ubiquitous Italian fashion brand)*
- *live.com (a Windows Live service that allows users to create a personalized homepage)*
- *livefilestore.com (Microsoft's Web Storage service)*
- *yellowpages.com (American telephone directory)*

Targeted news Websites were:

- *cnn.com (official Web site of the Cable News Network owned by Time Warner)*
- *msn.com and msnbc.com (a joint venture between NBC Universal and Microsoft for online news)*
- *bbc.co.uk (British Broadcasting Corporation's online news Website)*

Not only do these legitimate Web sites 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 e-mails.

Common Top Level Domains in URL Spam

The Top Level Domain .com dominates the domain table in the previous section. However, the analysis of Top Level Domains reveals another story of what sparks the interest of spammers. The following tables show the five most frequently used Top Level Domains used in spam by month:

Rank	January 2008	February 2008	March 2008	April 2008	May 2008	June 2008
1.	com	com	com	com	com	com
2.	cn (China)	cn (China)	net	net	cn (China)	cn (China)
3.	hk (Hong Kong)	hk (Hong Kong)	cn (China)	cn (China)	net	net
4.	net	net	info	biz	info	it (Italy)
5.	info	es (Spain)	be (Belgium)	info	tk (Tokelau)	uk (United Kingdom)

Table 14: Most Common Top Level Domains in Spam, 2008 H1

Rank	July 2008	August 2008	September 2008	October 2008	November 2008	December 2008
1.	com	com	com	com	com	com
2.	cn (China)	cn (China)	cn (China)	cn (China)	cn (China)	cn (China)
3.	net	net	info	net	net	ru (Russia)
4.	de (Germany)	org	net	biz	es (Spain)	net
5.	it (Italy)	info	org	org	ru (Russia)	es (Spain)

Table 15: Most Common Top Level Domains in Spam, 2008 H2

Aside from the generic Top Level Domains (.com, .net, .org, .biz), each month reveals some country-specific top-level domains (ccTLDs) that reach the top five, which are highlighted in the tables. Country-specific trends over time are more evident in the following charts. Figure 32 shows the TLDs with the highest volume, and Figure 33 shows second tier players. In the top tier players, China showed a significant increase towards the end of the year.

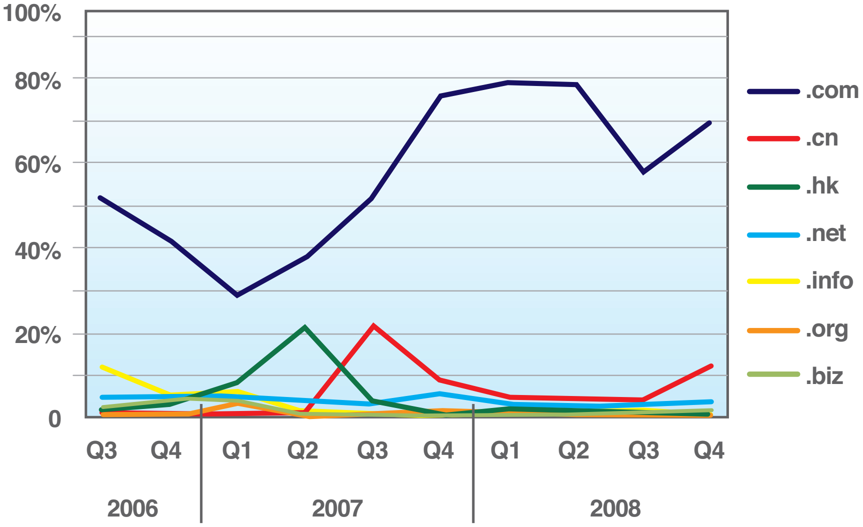


Figure 32: Percentage of Spam Using URLs of .com, .cn, .hk, .net, .info, .org, .biz

The Top Level Domains of some countries in some months reach the second league of most used Top Level Domains. However, the usage is much below the usage of .com and .cn as shown above. But the variety of different Top Level Domains used by spammers increases:

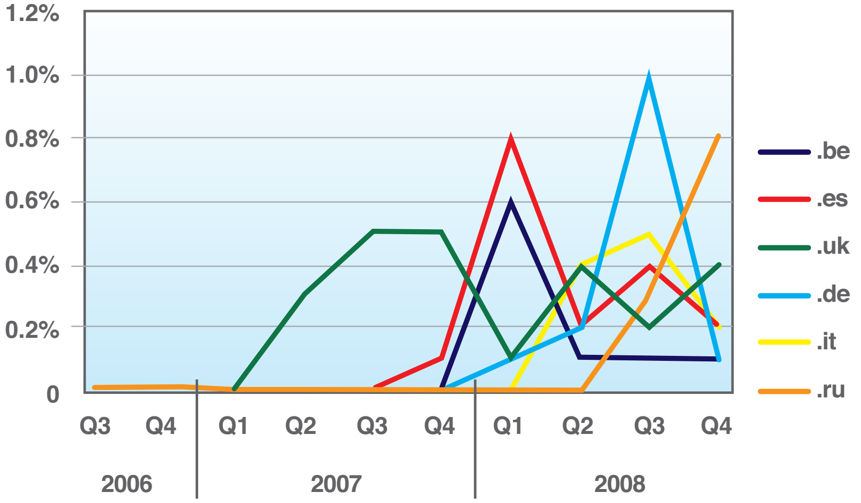


Figure 33: Percentage of Spam Using URLs of .be, .es, .uk, .de, .it, .ru

The usage of other generic or country code Top Level Domains is mostly below 0.1%.

Why .com? / Why .cn?

Using .com URLs in spam is the most unsuspicious type of URL because 55% of all domains used on the Internet are .com domains (source: IBM ISS data center, see Web Content Trends on page 87 for more details). However, spammers do not only use .com domains to host their spam content. They also use random .com URLs that are legitimate within their spam messages to make spam filters believe the message itself is legitimate. This trend became blatantly apparent in March, 2008 particularly, when we saw four times the amount of new .com domains used in spam in comparison to previous months. Upon further analysis, we discovered that this outlier month came from the usage of .com domains consisting of four characters (such as "abcd.com"). Thus, at first it seemed that spammers registered these domain names systematically. However, after comparing to these domains with the analysis from our Web crawler that supports our Web filtering technologies, it was apparent that these domains were registered years ago and were held as parking domains. The spammers did not register them. They simply used them alongside the real Spam URLs to make their messages appear to be more legitimate.

Another popular TLD was .cn. 10% of all Spam contained a .cn URL in the last quarter of 2008. One reason may be that it is cheap and easy to register a .cn domain. In some cases, spammers and phishers used a familiar .com domain with a .cn TLD instead. In comparison to other country TLDs, .cn might more easily visually trick unsuspecting users (compare "domain.com" with "domain.cn" vs. "domain.ru"). However, the predominant reason that we are seeing so many .cn TLDs is that a growing percentage of URL spam is directed at the Chinese.

Lifespan of Spam URLs

Over the past few years, the URLs that these spam messages point to have had a shorter and shorter lifespan. The quicker they are put up and taken down, the more likely they will avoid detection. Two and a half years ago, more than half of the URLs used in spam were up for longer than a month. At the end of 2008, more than 97 percent of these URLs are up a week or less as shown in Figure 34. Although this trend towards shorter lifecycles has been progressing for some time, it is now much more relevant with the onslaught of URL-based spam that has happened over the past year.

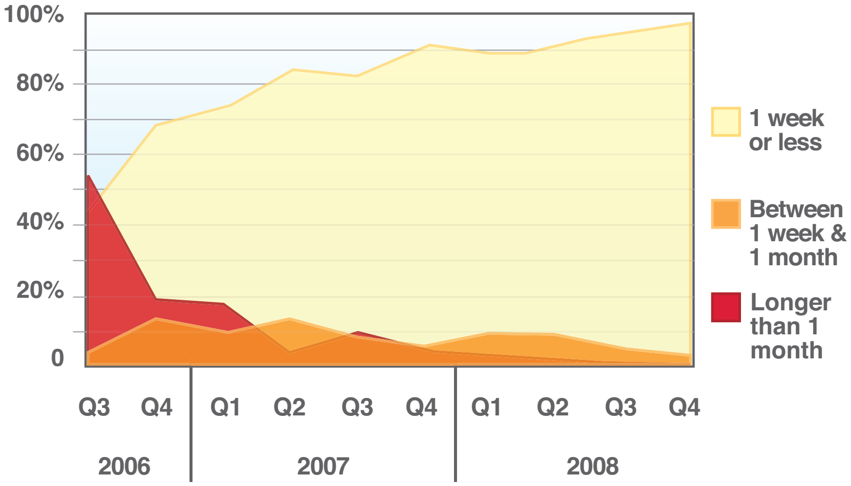


Figure 34: Lifespan of Spam URLs

Spam – Country of Origin

The following map shows the origination point[2] for spam globally in 2008.

The following map shows the origination point for spam globally. Russia, the U.S., and Turkey account for about 30% of worldwide spam.

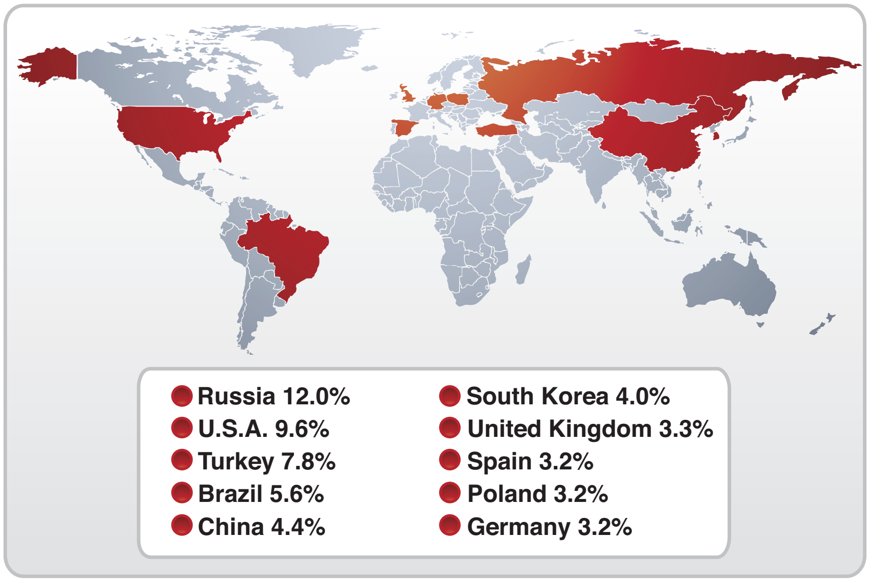


Figure 35: Geographical Distribution of Spam Senders

[2] *The country of origin indicates the location of the server that sent the spam e-mail. X-Force believes that most spam e-mail is sent by bot networks. Since bots can be controlled from anywhere, the nationality of the actual attackers behind a spam e-mail may not be the same as the country from which the spam originated.*

Spam – Country of Origin Trends

Over the last three years, spam originating from servers in Russia, Turkey, and Ukraine has increased. Furthermore, several countries (Brazil, China, and the UK) have had slower, but sustained growth.

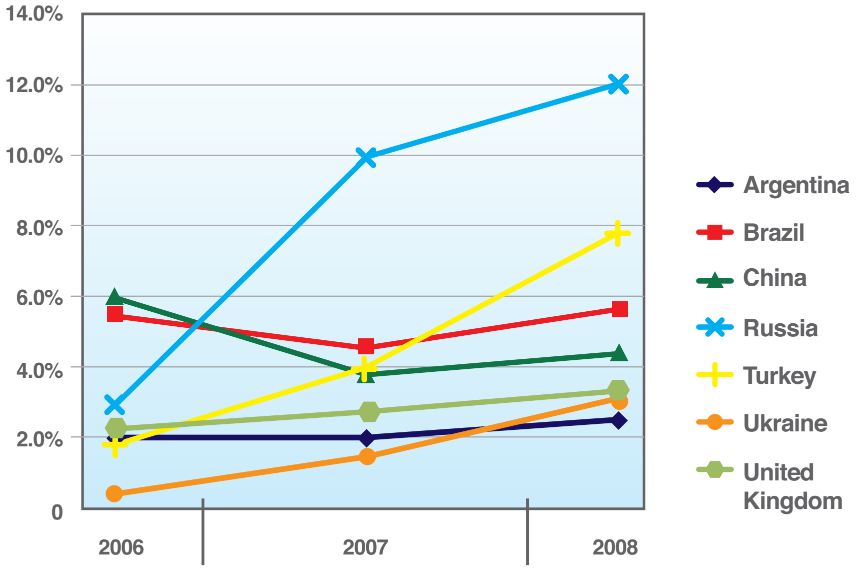


Figure 36: Spam Origin Trends, Long-Term Gainers and Sustainers

In contrast, several countries have declined, as shown in Figure 37:

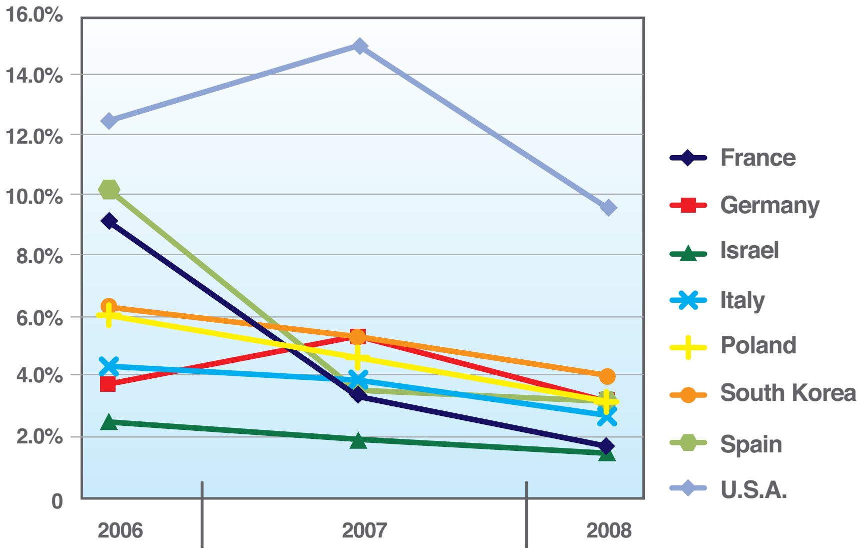


Figure 37: Spam Origin Trends, Long-Term Decliners

Spam URLs – Country of Origin

The following map shows where the spam URLs are hosted.

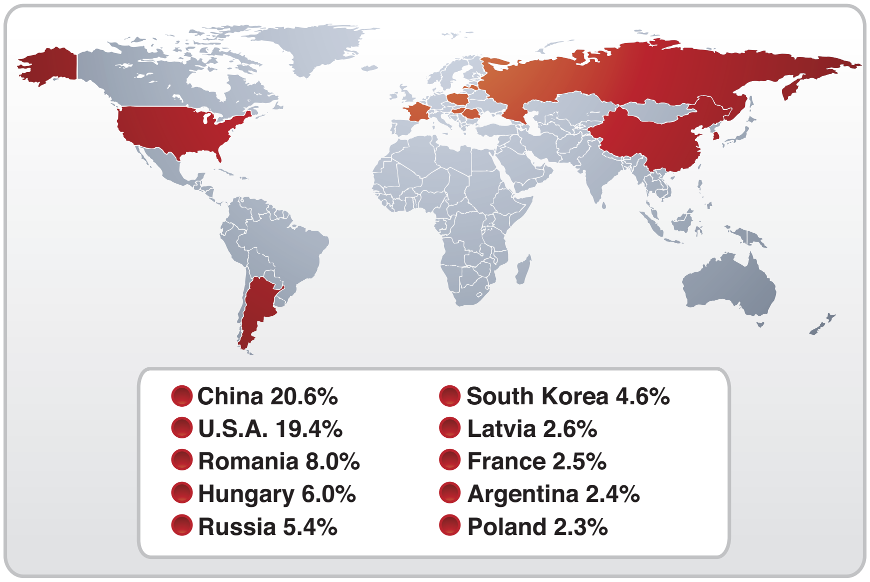


Figure 38: Geographical Distribution of Spam URLs

Spam URLs – Country of Origin Trends

Over the last three years one can see a tendency towards spam content hosted in Russia and Romania while most of the other countries decline. China and the US still host the most spam content as shown in Figure 39. Figure 40 shows countries that have seen gradual increases over the past few years, and Figure 41 shows countries that hosted a significant percentage of spam URLs in the past, but are now much less active.

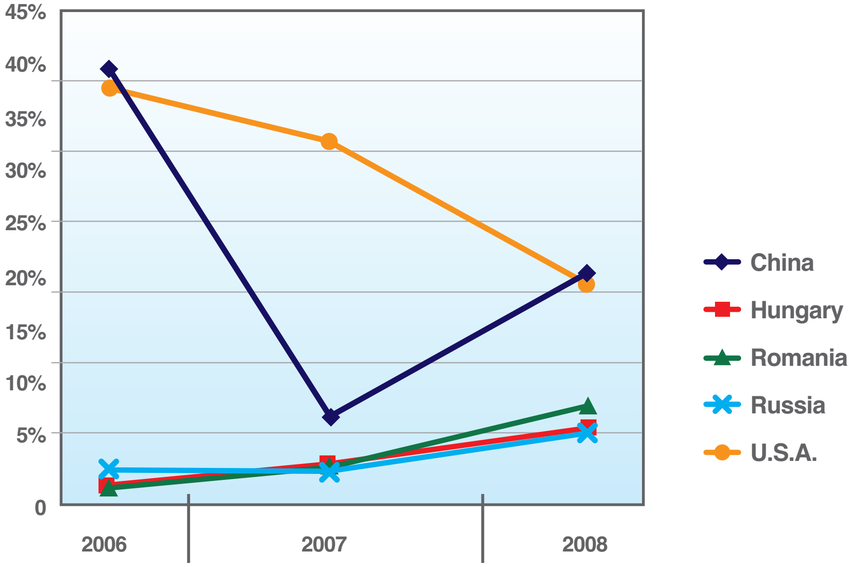


Figure 39: Spam URL Hosts, Major Contributors

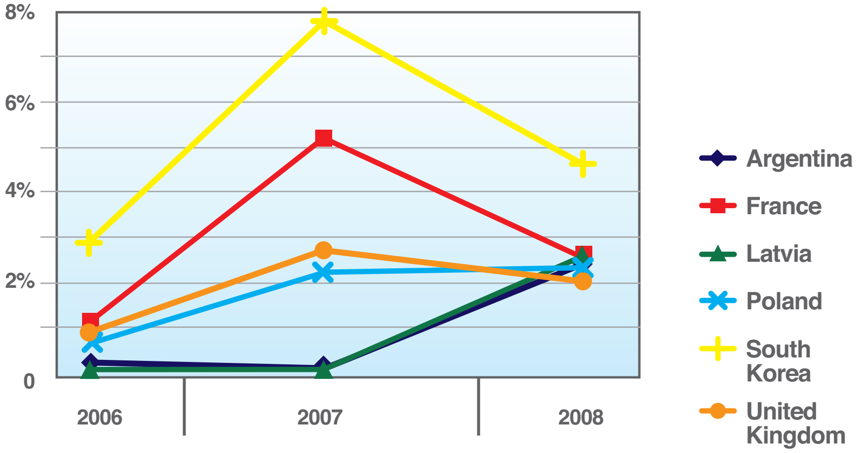


Figure 40: Spam URL Hosts, Long-Term Gainers and Sustainers

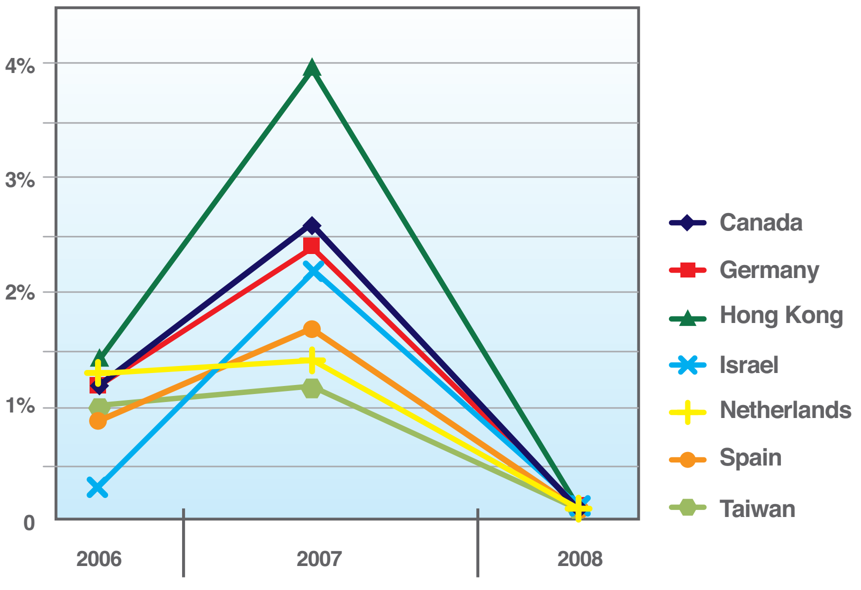


Figure 41: Spam URL Hosts, Long-Term Decliners

Spam – Average Byte Size

The most significant change in the average byte size of Spam happened at the end of 2007 and corresponded with the decline of image-based Spam. In 2008, byte size began to rise ever so slightly up until the McColo takedown later in the year.

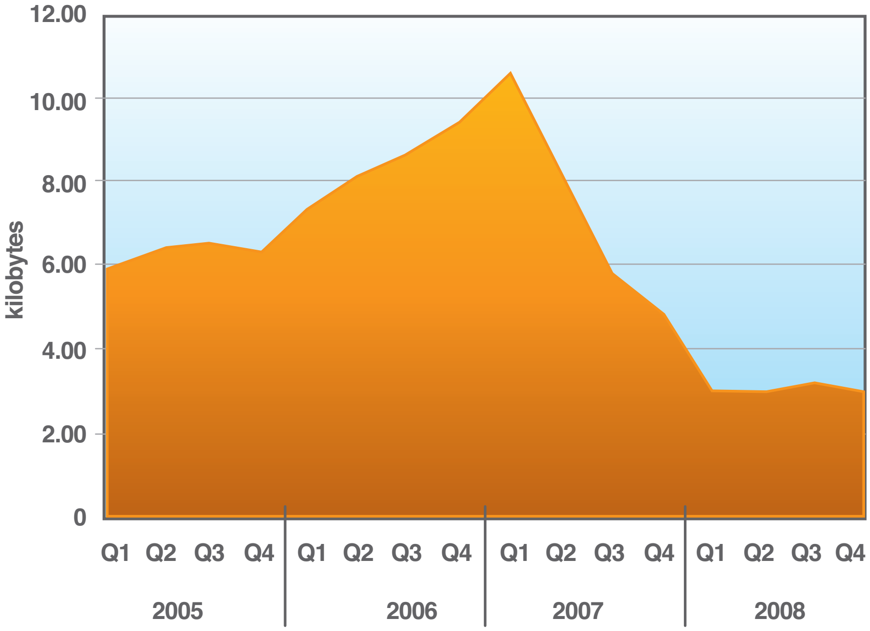


Figure 42: Average Byte Size of Spam Since 2005

Spam – Most Popular Subject Lines

Like phishing subject lines, spam subject lines are becoming more and more granular. The top ten subject lines of 2008 take up a much smaller percentage of the overall spam volume in comparison to 2007. As shopping on the Internet becomes more and more popular, spammers use subjects about an order's status to attract the user's interest. Furthermore, the offer of replica watches and free pornographic DVDs appear to be a popular attention-grabber. Most of the other top ten subject lines, are not especially indicative of any particular trend except for the "CNN Alerts" subject which corresponds to the trend of using news URLs in spam, described in Common Domains in URL Spam on page 58.

The following table shows the most popular spam subject lines in 2007 and 2008:

2007 Subject Lines	%	2008 Subject Lines	%
Re:	7.18%	Your order	0.43%
<empty subject line>	2.78%	Re: Order status	0.41%
The Pharmacy America Trusts	2.12%	RE: Message	0.41%
The United States National Medical Association	1.47%	Replica Watches	0.41%
Fw:	1.47%	Re:	0.38%
Replica Watches	1.12%	Free porno DVD's to download	0.23%
Man Lebt nur einmal - probiers aus !	0.97%	Downloadable porno DVD's for free	0.23%
Can you tell me what's wrong, and how we can fix it?	0.96%	Exquisite Replica	0.22%
You've received an ecard from a Partner!	0.85%	CNN Alerts: My Custom Alert	0.18%
You've received a greeting ecard from a Worshipper!	0.81%	Hi	0.16%

Table 16: Most Popular Spam Subject Lines

The McColo Takedown and It's Impact on Spam

After the takedown of the California-based Web hoster McColo, we have noticed some significant changes in our spam activity. From a spam perspective, everyone has noted the overall drop. After the November 11th takedown, spam volume in our spam traps was down to around 25% of previous levels. More interesting, perhaps, is the marked change we noticed in the origins of spam (the country location of the spam bot, generally). While McColo was operated out of the United States, the sudden and extreme volume and country distribution changes observed after the shutdown point to McColo as the base operator of spam bots all around the world.

Changes in International Distribution of Spam

The United States has, for years, maintained a top spot in the spam origin list (see above). Six days before the takedown, it was in the number one spot:

Top 5 Countries Before		Top 5 Countries After		Top 5 Countries at End of 2008	
USA	14.2%	China	12.7%	Brazil	11.7%
Russia	11.0%	Russia	11.4%	USA	8.1%
Turkey	7.4%	USA	8.0%	China	6.6%
Spain	5.9%	South Korea	6.2%	Turkey	5.7%
Brazil	4.8%	Brazil	5.8%	Russia	5.7%

Table 17: Top Spammers Before and After the McColo Takedown

Six days after the takedown, spam production coming out of the US was reduced to a mere 14% of its original capacity. So, it was not a terrible surprise when the US finally lost its top spot on the list on this sixth day after the takedown.

We took a closer look at the impact of spam around the globe, and the McColo takedown had a significant impact on countries that you might not expect. For example, spam production coming out of Spain, India, Italy, Israel, and Turkey were all reduced to less than 17% of their original production capacity. Other countries were also affected, albeit to a lesser extent, as shown in the graph below:

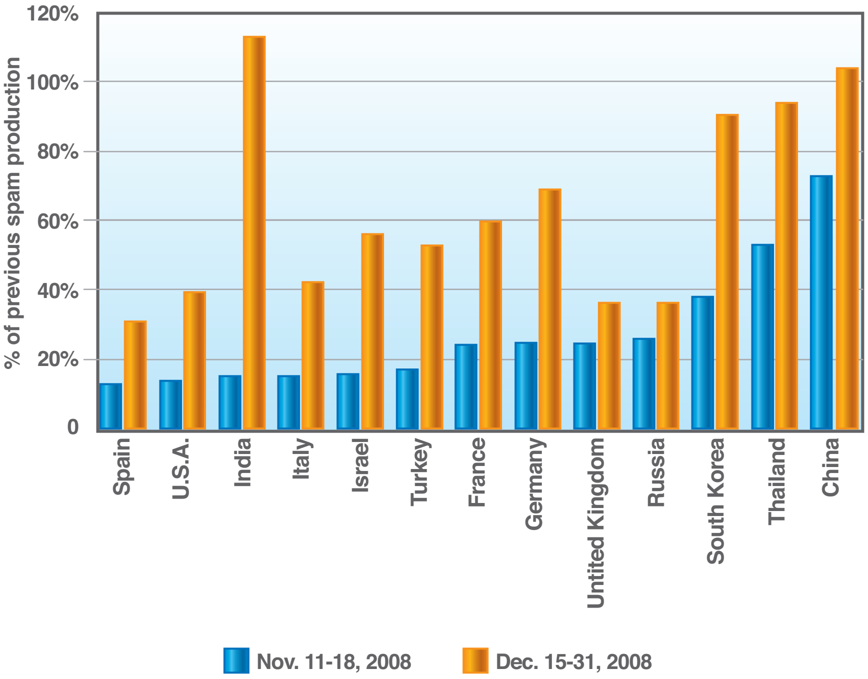


Figure 43: Spam Reduction by Country After the McColo Takedown – Nov. 11 – 18, 2008

The second bar in Figure 43 shows which countries have had the fastest recovery from the loss. While India and China have completely recovered from the loss, and Thailand and South Korea have nearly recovered completely, many other countries still produce significant less spam than before the shutdown.

Changes in Spam Content

Additional changes were reflected in the overall volume and also the type of spam sent out. Spammers were forced to find new ways to compensate for their losses. In the first few days, very little changed. Spam volume was simply down. The changes in spam types started showing up a few days later as the following figure demonstrates.

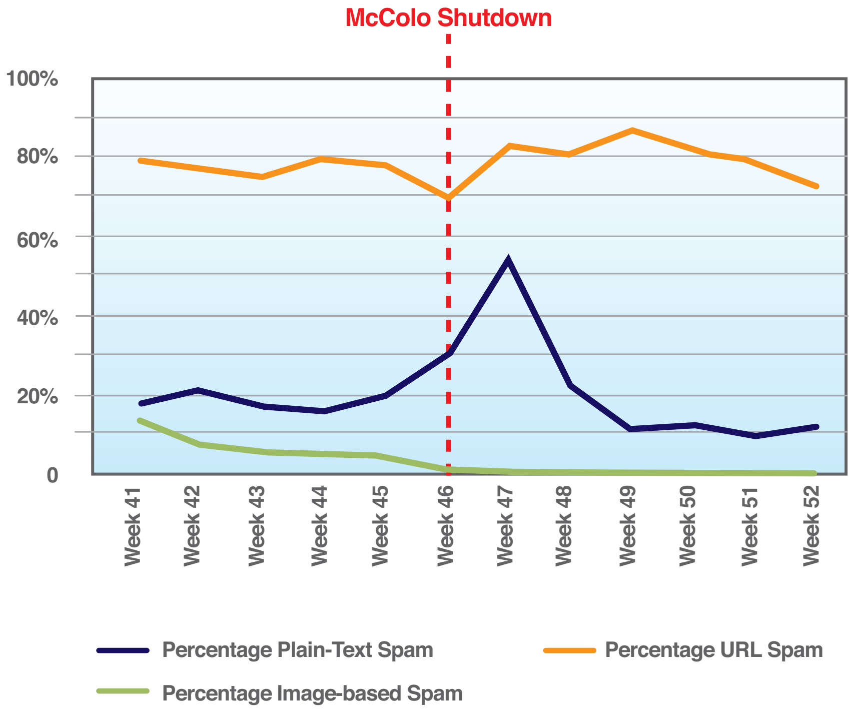


Figure 44: Spam Type Changes after the McColo Takedown

After the shutdown, the spammers switched to simple, plain-text spam (without HTML or attachments) within a few days, which reversed the trend at the time as seen in Figure 44. Furthermore, they relied more heavily on URL spam (before the shutdown the percentage of URL spam was below 80 percent, after the shutdown it was above 80 percent). Spammers also stopped sending out Image-based spam. It is possible that the switch to plain-text spam could have provided spammers the quickest way to get out new spam under these significantly different circumstances. The overhead of creating extravagant images and HTML layouts may have been too much too organize and distribute.

Another reason could have been that the spammers wanted to use the limited capacities to send out as much spam as possible. Thus, they bet on smaller (plain-text or URL) spam because of bandwidth issues. These trends are also evident in the analysis of the average byte size of spam during this timeframe:

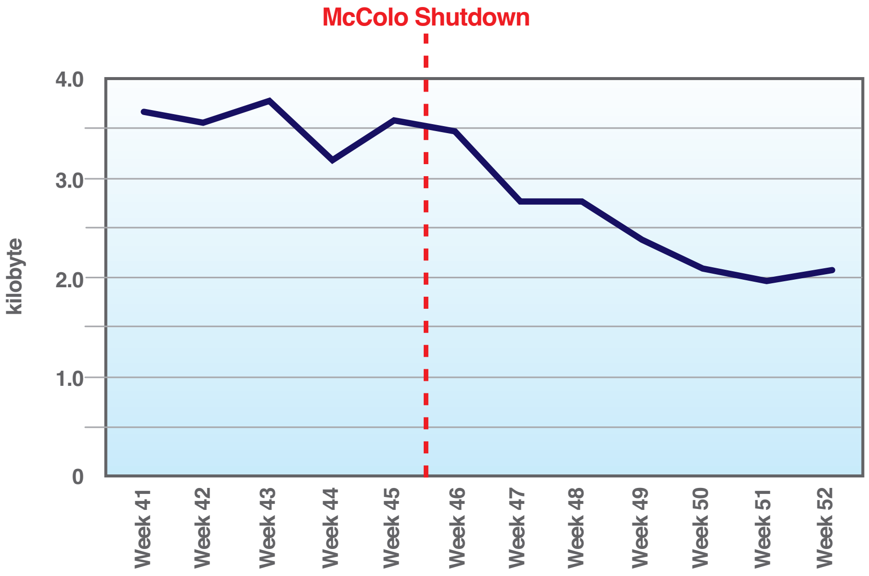


Figure 45: Average Byte Size of Spam Before and After the McColo Takedown

Only two weeks after the shutdown of McColo, the spam volume started to increase. If the trend continues (and from the old rates of growth of the spam volume it will continue) the prior level of spam volume will probably be reached early in the first quarter of 2009.

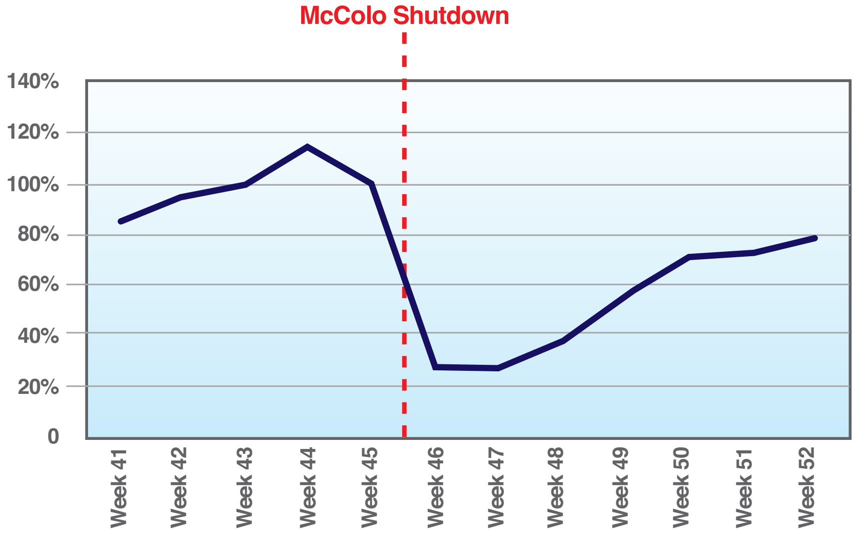


Figure 46: Spam Volume Before and After the McColo Takedown

In summary, there were two main phases after the McColo shutdown (November 11th, 2008):

- *First phase (November 12th until November 23rd): Short term actions taken by spammers like an increase in simple, plain-text spam and cessation of Image-based spam, although these changes did not impact on spam volume, which remained low for nearly two weeks.*
- *Second phase (since November 24th, still going): Reduction in the byte size of spam to spare bandwidth and to increase spam volume. Around Christmas, the rate of volume increase slowed slightly, but it still continuing to climb.*

For more information see http://blogs.iss.net/archive/mccolo.html and http://blogs.iss.net/archive/mccolo-2.html.

Phishing

This section covers the following topics:

- *Phishing as a percentage of spam*
- *Phishing country of origin trends, including phishing Web pages (URLs)*
- *Most popular subject lines and targets of phishing*

Phishing Volume

Throughout 2008, phishing volume was, on average, 0.5 percent of the overall spam volume. The percentage of spam that is phishing is between 0.4 percent and 1 percent with a decrease towards 0.2 percent in the second quarter of 2008 but an increase towards 0.8 percent in the second term of 2008. Obviously, Phishers used the financial crisis and the uncertainty of bank customers to send out targeted phishing this year. The decline in the last quarter is most likely tied to the McColo shutdown.

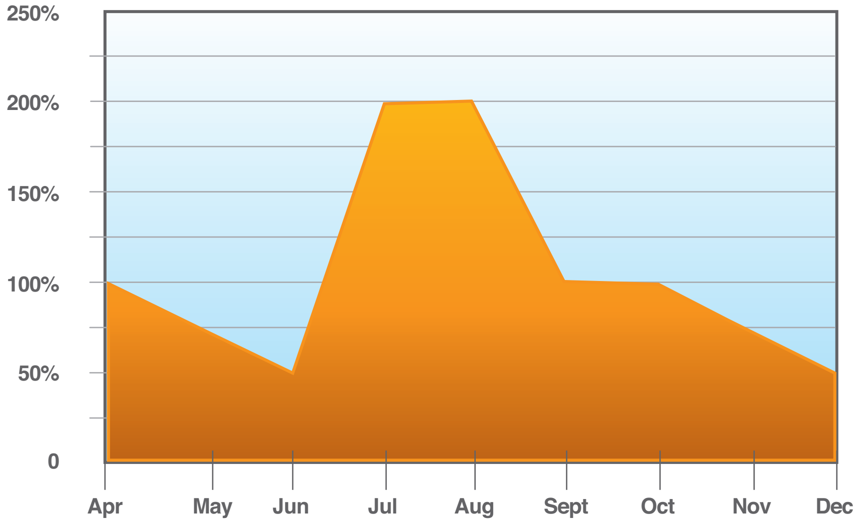


Figure 47: Phishing Volume Changes Over 2008

Phishing – Country of Origin

The following map highlights the major countries of origin for phishing emails in 2008.

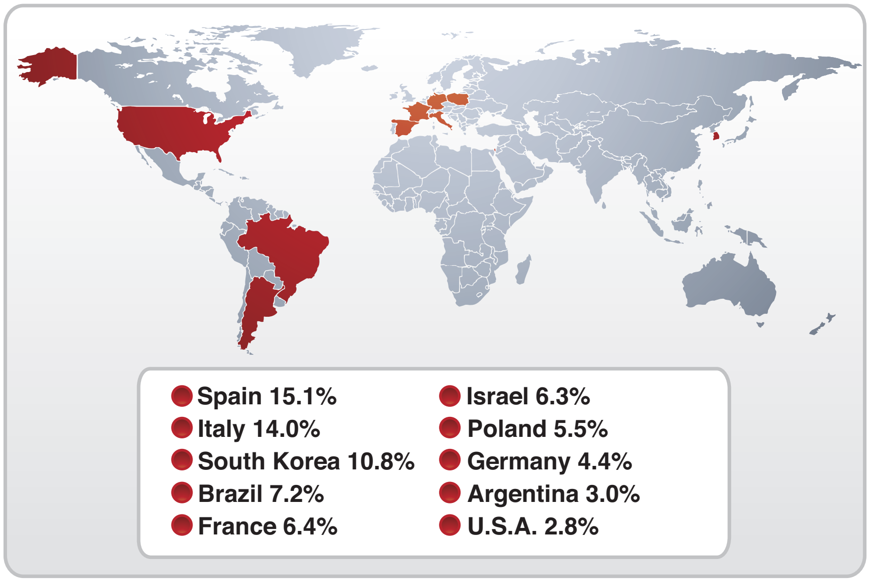


Figure 48: Geographical Distribution of Phishing Senders

Phishing – Country of Origin Trends

Over the past three years, Italy and Korea have emerged as leading phishing senders, while Spain remains the uncontested top origin of phishing emails. Israel and Brazil, although declining slightly in 2008, are still major sources of phishing emails.

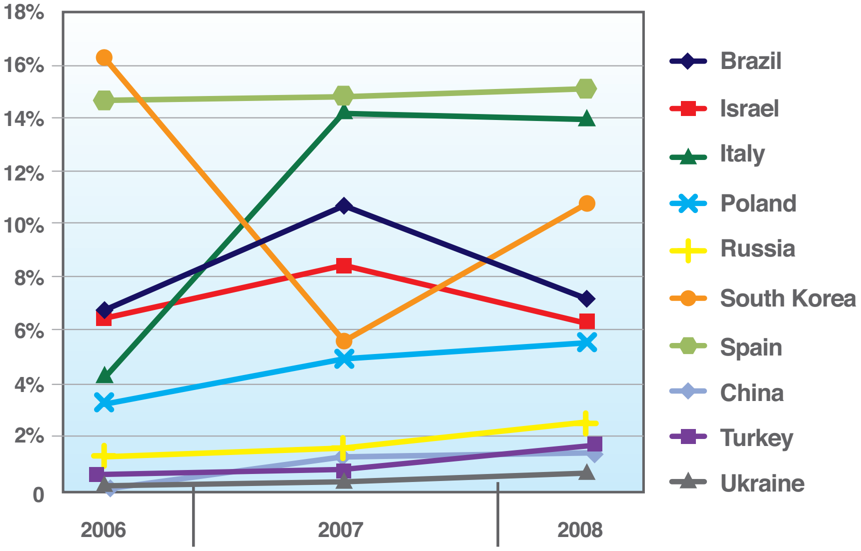


Figure 49: Phishing Origin Trends: Long-Term Gainers and Sustainers

Several countries have shown significant declines as phishing sources, especially the US and France.

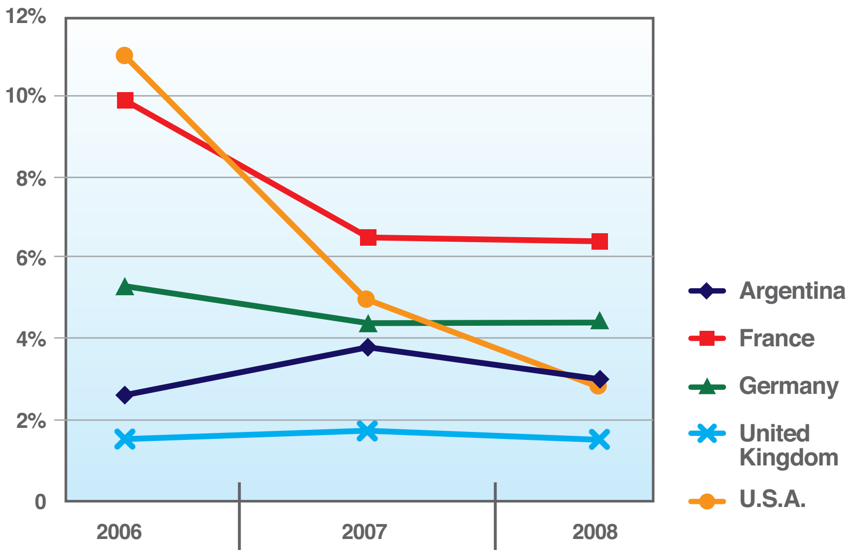


Figure 50: Phishing Origin Trends: Long-Term Decliners

Phishing URLs – Country of Origin

The following map shows where the Phishing URLs are hosted.

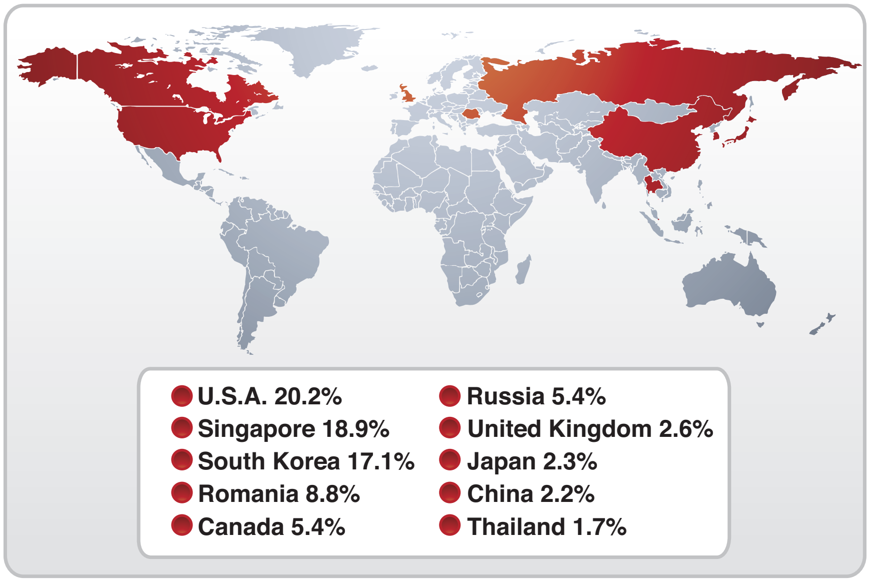


Figure 51: Geographical Distribution of Phishing URLs

Phishing URLs – Country of Origin Trends

Over the last three years, there have been many changes in the major Phishing URL hosting countries: While the US has dramatically declined, it still remains the top host of Phishing URLs, but just barely – Singapore and South Korea are not far behind:

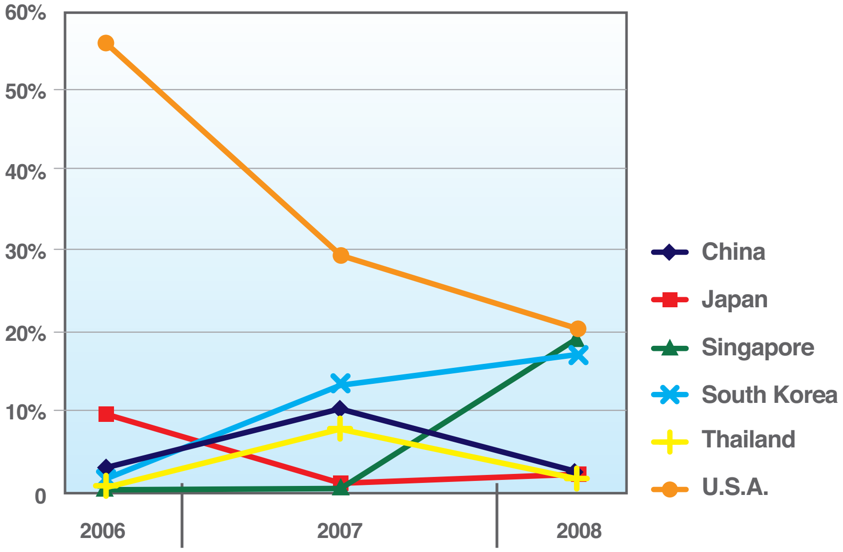


Figure 52: Phishing URL Hosts, Major Contributors

Other countries to watch are Romania, Canada, and Russia. These countries have shown significant increases over the past year:

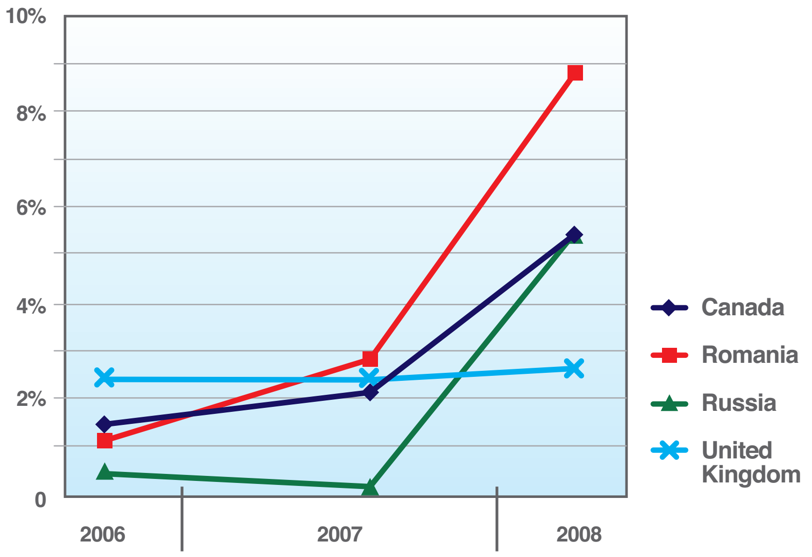


Figure 53: Phishing URL Hosts: Long-Term Gainers and Sustainers

Several countries have had significant declines in the number of Phishing URL hosts – most notably Kazakhstan and Germany:

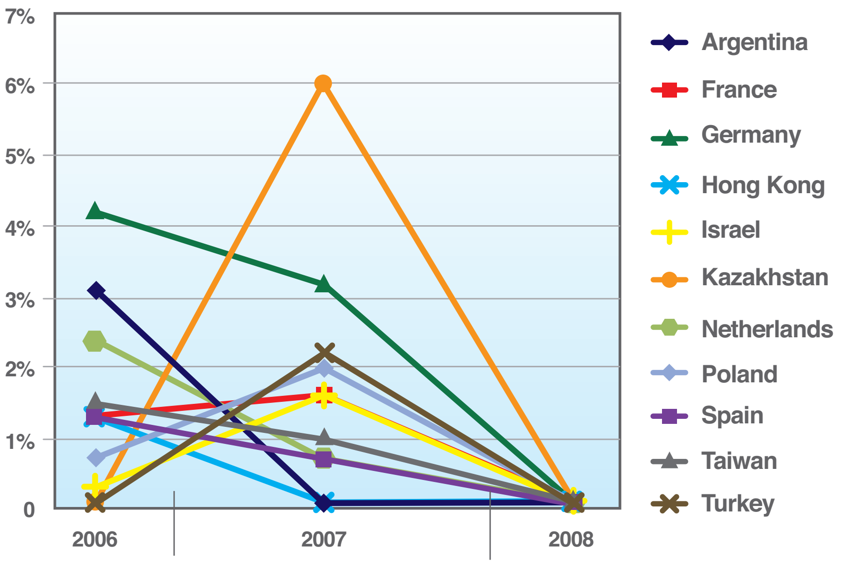


Figure 54: Phishing URL Hosts: Long-Term Decliners

Phishing – Most Popular Subject Lines

One of the biggest changes in 2008 is that popular subject lines are not so popular anymore. In 2007, the most popular subject lines represented about 40% of all phishing emails. In 2008, the most popular subject lines made up only 6.23% of all phishing subject lines. The implication is that phishers are becoming more granular in their targets, essentially with a greater variance of subject lines than ever before. Another trend that developed in 2008 is the focus on user action. Rather than having a generic subject like "security alert," the phishers attempt to engage the user into doing something, like fixing an account that has been suspended or updating their account information.

The following table shows the most popular phishing subject lines in 2007 and 2008:

2007 Subject Lines	%
<empty subject line>	22.21%
Account Security Measures!	3.86%
Important Notice – E*TRADE FINANCIAL Corp	3.21%
Important Notice!	2.01%
Volksbanken Raiffeisenbanken AG: 02/11/2007	1.94%
Security Measures!	1.82%
Citibank Account Security!	1.77%
Citibank Bank Notice!	1.75%
Citibank Account Security Measures!	1.74%
Volksbanken Raiffeisenbanken AG: 14/11/2007	1.32%

2008 Subject Lines	%
PayPal® Account Review Department	1.47%
PayPal Security Department	0.97%
PayPal Abuse Department.	0.63%
PayPal Account Security Measures	0.60%
Volksbanken Raiffeisenbanken	0.48%
PayPal Account Suspention	0.47%
Restore Your Barclays Account	0.44%
Read carefully - Important Notification	0.40%
Update Your Billing Information.	0.39%
Read carefully - Important Notification!	0.38%

Table 18: Most Popular Phishing Subject Lines

Phishing Targets

Phishing – Targets by Industry

In 2008, the majority of phishing – nearly 90 percent – was targeted at financial institutions. Seven percent targeted online payment services and less than five percent targeted other industries (like online auction Websites, communication services, and online stores):

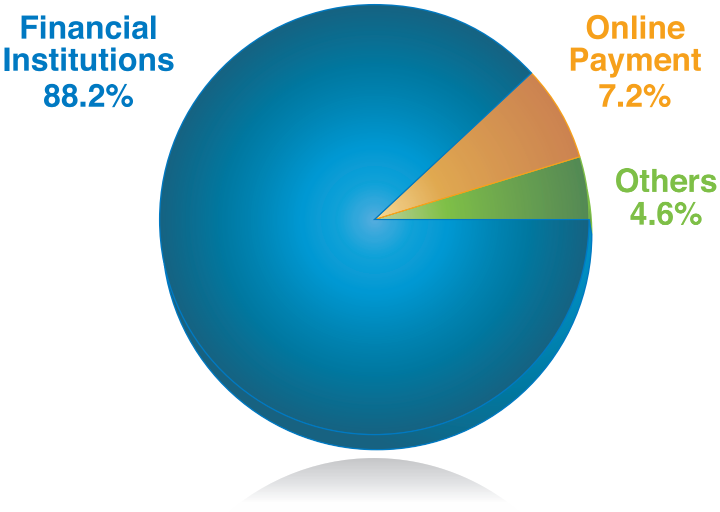


Figure 55: Phishing by Industry, 2008

Phishing – Financial Targets by Geography

Over 99% of all financial phishing targets are in North America or Europe, with the majority of targets in North America (58.4 percent):

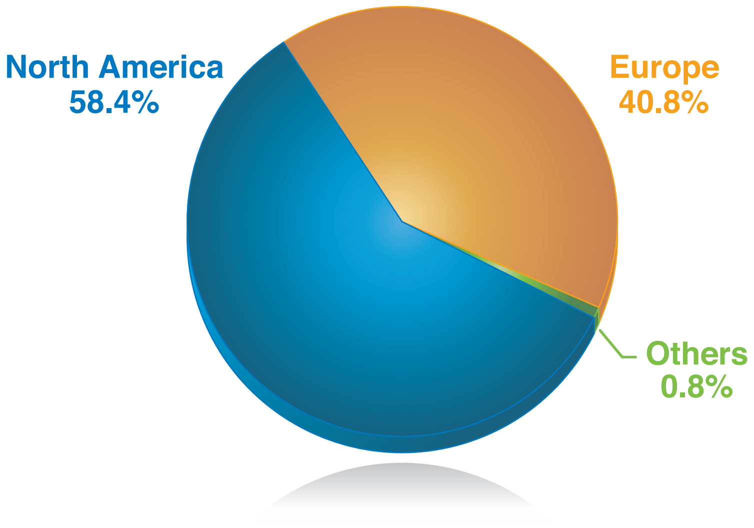


Figure 56: Financial Phishing by Geographical Location, 2008

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 Web sites: adult, social deviance and criminal. Table 19 lists the IBM ISS Web filter categories that correspond with these types of sites.

The Web filter categories are defined in detail at:

http://www.ibm.com/services/us/index.wss/detail/iss/a1029077?cntxt=a1027244

Web Site 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 19: Web Filter Categories Associated with Unwanted Web Content

This section provides analysis for:

- *Percent and distribution of Web content that is considered bad, unwanted, or undesirable*
- *Percent and distribution of adult content*
- *Percent and distribution of socially deviant content*
- *Percent and distribution of criminal content*
- *Increase in the amount of anonymous proxies*

Analysis Methodology

X-Force captured information about the content distribution on the Internet by counting the hosts categorized in the IBM ISS Web filter database. Counting hosts is an accepted method for determining content distribution and provides the most realistic assessment. When using other methodologies – like counting Web pages/sub pages – results may differ.

The IBM ISS data center is constantly reviewing and analyzing new Web content data. Consider the following statistics related to the IBM ISS data center:

- *Analyzes 150 million new Web pages and images each month*
- *Has analyzed 9.1 billion Web pages and images since 1999*

The IBM ISS Web Filter Database has:

- *68 filter categories*
- *100 million entries*
- *150,000 new or updated entries added each day*

Percentage of Unwanted Internet Content

Currently, about 8 percent of the Internet contains unwanted content such as pornographic or criminal Web sites.

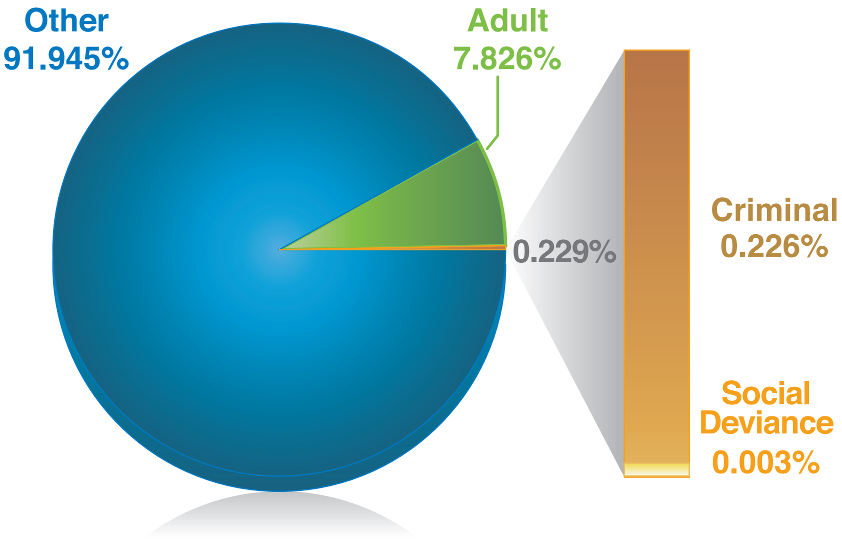


Figure 57: Content Distribution of the Internet, 2008

Geographical Distribution of Adult Content

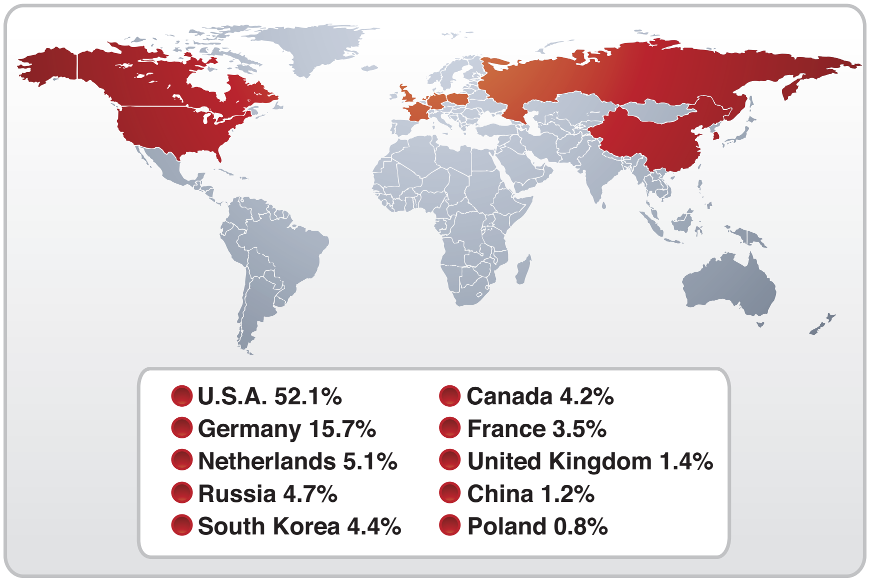


Figure 58: Geographical Distribution of Adult Content

Geographical Distribution of Socially Deviant Content

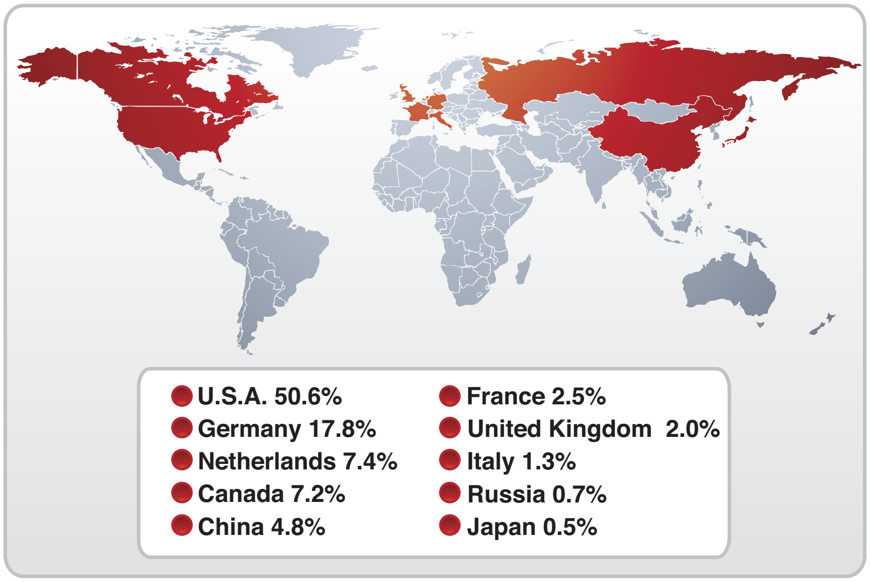


Figure 59: Geographical Distribution of Socially Deviant Content

Geographical Distribution of Criminal Content

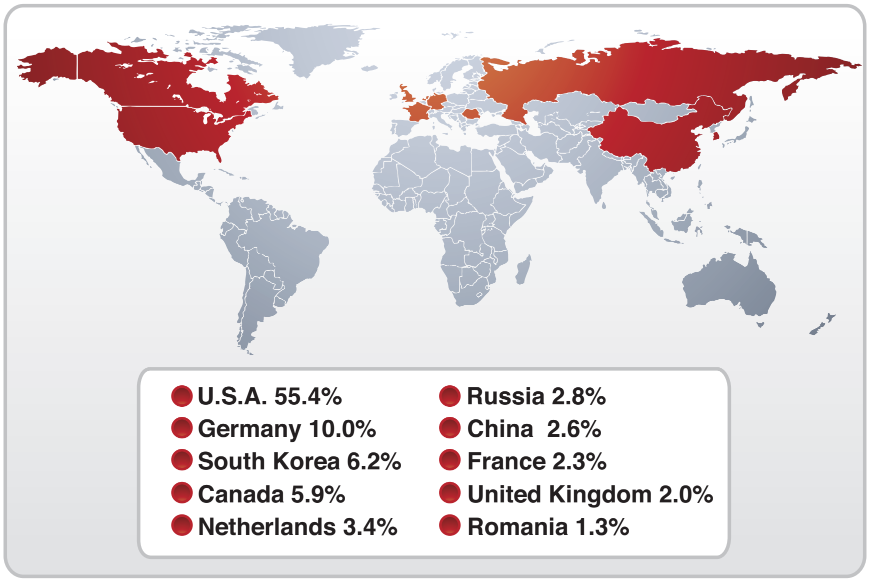


Figure 60: Geographical Distribution of Criminal Content

Increase of Anonymous Proxies

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

One such control is a content filtering system that prevents access to unacceptable or inappropriate Web sites as described in this section of the Trend Report. In an effort to circumvent Web filtering technologies, some individuals might attempt to use an Anonymous Proxy (also known as Web Proxy).

Web proxies allow users to enter an URL on a Web form instead of directly visiting the target Web site. Using the proxy hides the target URL from a Web filter. If the Web filter is not also set up to monitor or block Anonymous Proxies, then this activity, which would have normally been stopped, will bypass the filter and allow the user to reach the disallowed Webpage.

The rate of increase of Anonymous Proxy Web sites reflects this trend:

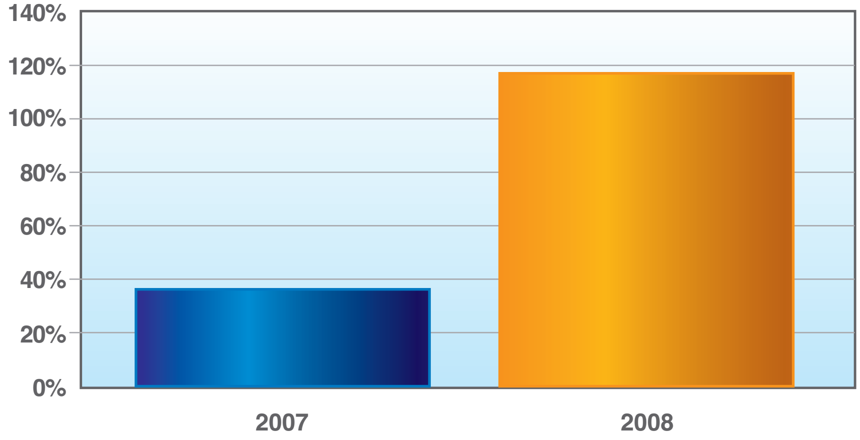


Figure 61: Year Over Year Increase of Anonymous Proxy Web Sites

In 2007, the number of anonymous proxies increased by about 1/3. In 2008, they more than doubled in comparison to 2007.

Malware Trends

Malware Category Trends

The following chart shows the percentage of malware falling into each major category for 2008:

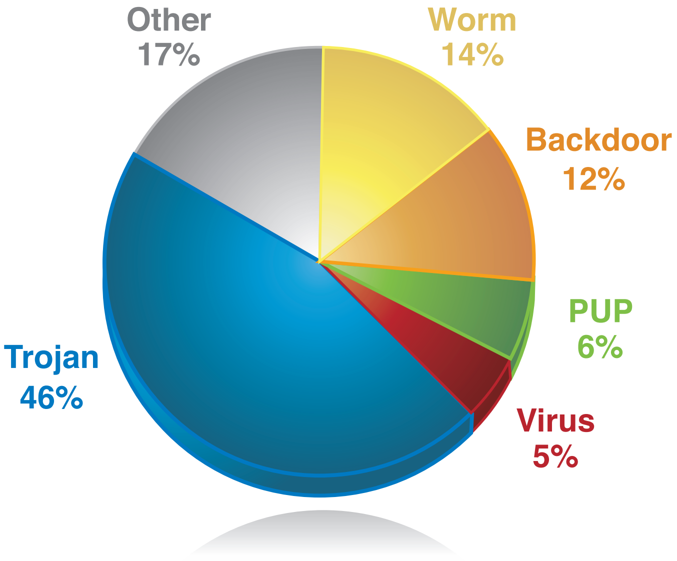


Figure 62: Malware by Category, 2008

The primary malware categories are:

- ***Virus*** *– Propagates by infecting a host file.*
- ***Worm*** *– Self-propagates through e-mail, network shares, removable drives, file sharing or instant messaging applications.*
- ***Backdoor*** *– Provides functionality for a remote attacker to log on and/or execute arbitrary commands on the affected system.*
- ***Trojan*** *– Performs a variety of malicious functions such as spying, stealing information, logging key strokes and downloading additional malware.*
- ***Potentially Unwanted Programs (PUP)*** *– Programs which the user may consent on being installed but may affect the security posture of the system or may be used for malicious purposes. Examples are Adware, Dialers and Hacktools/"hacker tools" (which includes sniffers, port scanners, malware constructor kits, etc.)*
- ***Other*** *– Unclassified malicious programs not falling within the other primary categories.*

Trojan Functionality Breakdown

Since a large percentage of malware was classified as Trojans in 2008, it is important to consider how the functionality of these Trojans varies. The data below shows the breakdown and trend of the Trojan category for 2008.

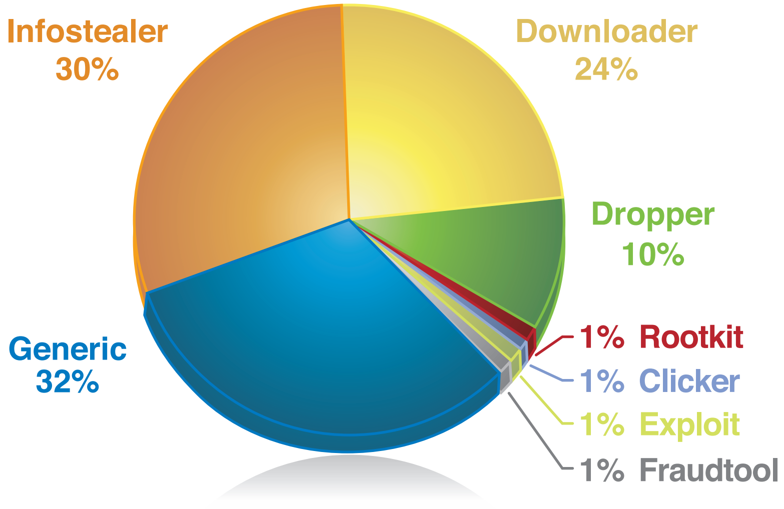


Figure 63: Trojans by Category, 2008

The Trojan subcategories are as follows:

- ***Infostealer*** *– Spies and/or steals information; this includes password stealers, keystroke loggers and spyware.*
- ***Downloader*** *– Downloads one or more malware components from a remote site and then installs them on the affected system.*
- ***Dropper*** *– Drops and installs one or more malware components into an affected system.*
- ***FraudTool*** *– Malware used to commit fraud, an example of which is malware that displays fake error or infection messages which then entices the user to purchase fake tools or security software.*
- ***Clicker*** *– Generates Website traffic, the purpose of which is to generate revenue or other malicious purposes.*
- ***Rootkit*** *– Components used by other malware in order to have the capability to hide themselves from the user and security software.*
- ***Exploit*** *– Documents or media files containing exploit code.*
- ***Proxy*** *– Allows a remote attacker to relay connections through the affected system in order to hide its real origin.*
- ***Generic*** *– Trojans that do not fall within the other subcategories.*

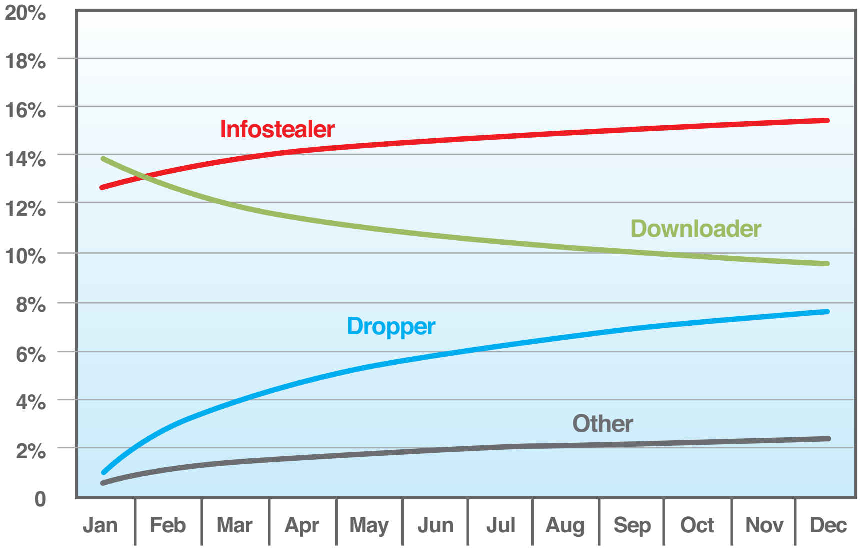


Figure 64: Trojan Trends, 2008

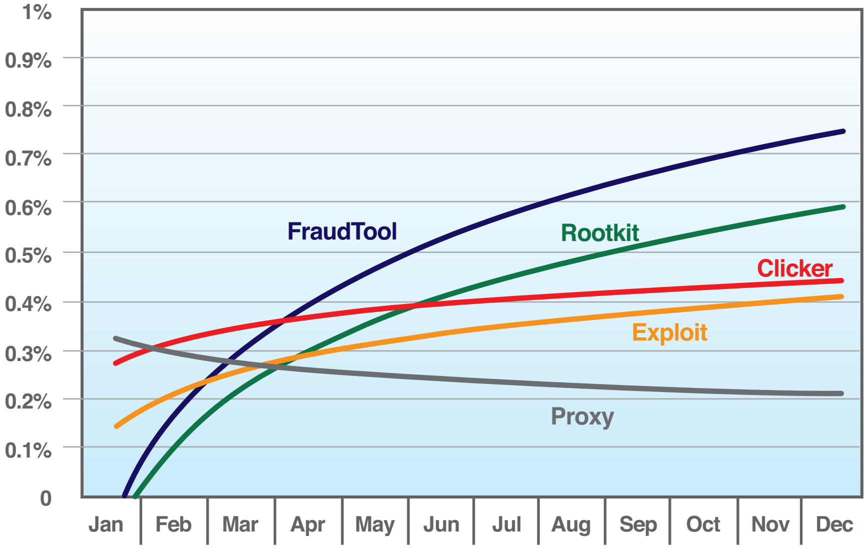


Figure 65: Trojan Trends, Granular Detail for Other Category, 2008

Analysis and Findings

- *The most prevalent malware category is Trojan which comprises 46% of our malware collection*
- *The most common Trojan subcategories (excluding the Trojan-Generic subcategory) are Infostealers (30%), followed by Downloaders (24%) and Droppers (10%). The trend also shows that the proportion of Infostealers and Droppers had increased throughout the year.*
- *The prevalence of Infostealer Trojans suggests that attackers continually aim to spy and steal information from users. A large percentage of these Infostealer Trojans are those that target online games (38% of Infostealers) and online banking users (18% of Infostealers).*
- *The prevalence of Downloaders and Droppers suggests continued use of multi-component/multi-stage strategy in which additional malware components are either downloaded or dropped after the affected system is compromised.*

Prevalent Malware Families

The table below lists the most common malware families for 2008; generic families such as Agent or Delf are not included in the list:

Rank	Family	Category
1	Allaple	Worm
2	Onlinegames	Trojan-Infostealer
3	Virut	Virus
4	Hupigon	Backdoor
5	Banker	Trojan-Infostealer
6	Swizzor	Trojan-Downloader
7	Banload	Trojan-Downloader
8	Ardamax	Trojan-Infostealer
9	Bifrose	Backdoor
10	Rbot	Backdoor
11	Ldpinch	Trojan-Infostealer
12	Poison	Backdoor
13	Zlob	Trojan-Downloader
14	Kgen	Trojan-Dropper
15	Autorun	Worm
16	Ircbot	Backdoor
17	Virtumonde	PUP-Adware
18	Magania	Trojan-Infostealer
19	Adultbrowser	PUP-Dialer
20	Bagle	Trojan-Downloader

Table 20: Most Prevalent Malware Families, 2008

Analysis and Findings

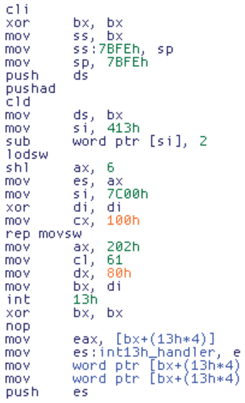
- *These top 20 most prevalent malware families comprise 35% of our malware collection.*
- *Allaple, a network worm which propagates through network shares and by exploiting vulnerabilities holds the number 1 position for 2008.*
- *Trojans targeting users of online games (Onlinegames, Magania) and online banking (Banker and Banload) remain prevalent for the whole year; which indicates that these specific user groups are highly targeted in 2008.*
- *All the backdoors (Hupigon, Bifrose, Poison, Rbot and Ircbot) included in the top 20 are families in which a constructor kit or source code is available.*
- *Aside from Allaple, the only other Worm that managed to be one of the top 20 is the Autorun Worm, suggesting that spreading through removable drives/devices continues to become a popular propagation method.*

Notable Malware Events in 2008

This section briefly discusses some of the notable malware events that happened in 2008.

MBR Rootkits

In the last weeks of 2007, a new malware named Mebroot (also known as Mbroot/StealthMBR) which uses a very old technique for stealth was first found in the wild[3] and additional variants of it were seen in 2008. An interesting capability of Mebroot is that it uses an old technique used by dated, stealth DOS boot viruses. Namely, it attempts to achieve stealth by placing its loader code into the MBR (Master Boot Record) so that it gains control of the system before the operating system and then redirects code (in this case, a driver dispatch routine) that is used for reading disk sectors so that when tools (like antivirus, for example) attempt to read the MBR, a clean MBR is presented to the tools instead. What is new, however, is that the technique was used against Windows NT-based operating systems. This development in malware/rootkit capabilities just showcases another example of adapting old techniques for new targets.



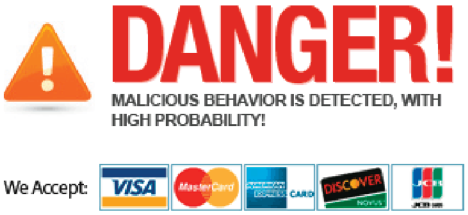
```
cli
xor     bx, bx
mov     ss, bx
mov     ss:7BFEh, sp
mov     sp, 7BFEh
push    ds
pushad
cld
mov     ds, bx
mov     si, 413h
sub     word ptr [si], 2
lodsw
shl     ax, 6
mov     es, ax
mov     si, 7C00h
xor     di, di
mov     cx, 100h
rep movsw
mov     ax, 202h
mov     cl, 61
mov     dx, 80h
mov     bx, di
int     13h
xor     bx, bx
nop
mov     eax, [bx+(13h*4)]
mov     es:int13h_handler, e
mov     word ptr [bx+(13h*4)
mov     word ptr [bx+(13h*4)
push    es
```

Figure 66: Initial instructions found in Mebroot's MBR code, bringing a nostalgic feeling of seeing boot viruses from the past

[3] http://www2.gmer.net/mbr/

Scareware Programs & Fake Antivirus

Scareware programs (classified as Trojan-FraudTool) also received the spotlight this year, because a large number of users had been reported to have been scammed by them. The scheme involves displaying fake error messages or malware detection messages, and then enticing the user into buying a full version of a fake tool or security program to fix these purportedly identified issues. The scheme usually starts with a user being redirected to Web sites that display these fake messages or Web sites offering a download of security software to scan the system (which in turn will display the fake messages). Additionally, malware installed on the system may also generate these fake messages. On December 2008, the Federal Trade Commission (FTC) issued an FTC consumer alert[4] for the scam and took legal actions[5] against some of the perpetrators. One way to avoid this scam is to know which vendors to trust. For example, consumers can look at the products being tested by notable AV testing firms such as AV-Comparatives, AV-Test, ICSA, or West Coast Labs. Additionally, a quick search for the name of the product in question can also reveal if it is a scam.



DANGER!

MALICIOUS BEHAVIOR IS DETECTED, WITH HIGH PROBABILITY!

Figure 67: Image Found in a Web Site Selling Fake Antivirus Software

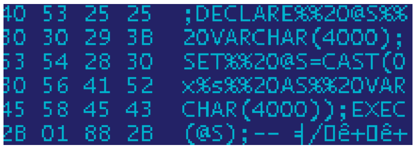
We expect this malware category to continue to rise in popularity because it is so effective. On the other hand, user awareness will also increase as more and more of these scams are brought into the spotlight.

[4] *http://ftc.gov/bcp/edu/pubs/consumer/alerts/alt121.shtm*

[5] *http://ftc.gov/opa/2008/12/winsoftware.shtm*

Botnets and SQL Injection Attacks

As discussed in the Web Application Vulnerabilities section of this report, we have seen mass SQL injection attacks, a portion of which is attributed to the Asprox botnet. This combination of a botnet plus a SQL injection attack capability enabled another method of mass delivery of malware in which a large number of affected sites effectively becomes a delivery point. Additionally, these automated attacks also highlighted the high number of Web sites vulnerable to SQL injection and that secure development practices[6] will go a long way in effectively mitigating these attacks.



```
40 53 25 25  ;DECLARE%%20@S%%
30 30 29 3B  20VARCHAR(4000);
53 54 28 30  SET%%20@S=CAST(0
30 56 41 52  x%s%%20AS%%20VAR
45 58 45 43  CHAR(4000));EXEC
2B 01 88 2B  (@S);-- ╡/□ê+□ê+
```

Figure 68: Part of a SQL Injection Attack String Template Used by the Asprox Botnet

Autorun Worms

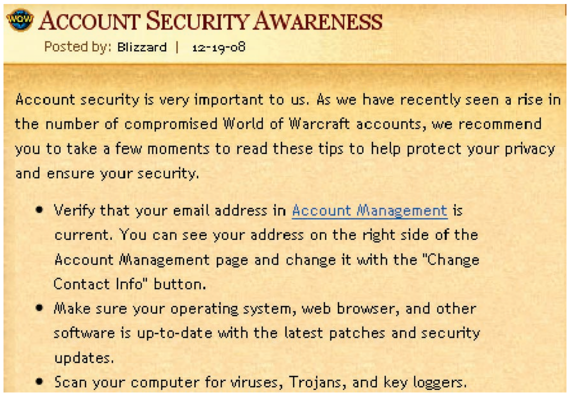
As we mentioned in our mid-year report, due to the continuing popularity of consumer devices such as MP3 players, external drives and digital picture frames, malware authors continue to seize the opportunity by using them as infection vector. One high profile case reported[7] on November 2008 involved federal government systems that were affected by such malware. Propagation through removable drives and taking advantage of the Autorun feature of Windows remains to be one of the most successful ways propagate. Having policies to control the use of external devices in corporate systems and disabling the Autorun feature of Windows would help mitigate infection against these types of malware.

[6] http://msdn.microsoft.com/en-us/library/ms998271.aspx

[7] http://blog.wired.com/defense/2008/11/army-bans-usb-d.html

Malware Targeting Online Game Users

Finally, this year, we had also seen an upsurge in the number of variants of malware targeting online game users. As we had seen in our top 20 most prevalent malware families for 2008, an Infostealer Trojan targeting online game users holds the number 2 position. Driven by the continued popularity of online games along with an underground economy for stolen virtual assets, we can expect that next year, there will be no slow down in the production of new malware variants targeting online game users.



ACCOUNT SECURITY AWARENESS

Posted by: Blizzard | 12-19-08

Account security is very important to us. As we have recently seen a rise in the number of compromised World of Warcraft accounts, we recommend you to take a few moments to read these tips to help protect your privacy and ensure your security.

- Verify that your email address in Account Management is current. You can see your address on the right side of the Account Management page and change it with the "Change Contact Info" button.
- Make sure your operating system, web browser, and other software is up-to-date with the latest patches and security updates.
- Scan your computer for viruses, Trojans, and key loggers.

Figure 69: Posting in the World of Warcraft Community Site on December 19, 2008

(Image source: http://www.worldofwarcraft.com/index.xml)

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America.
January 2009