A Websense® White Paper

Websense Security Labs

State of Internet Security, Q3 – Q4, 2008

websense®
ESSENTIAL INFORMATION PROTECTION™

Key Findings

Websense® Security Labs™ uses the patent-pending Websense ThreatSeeker™ Network to discover, classify, and monitor global Internet threats and trends. Featuring the world's first Internet HoneyGrid™, the system uses hundreds of technologies including honeyclients, honeypots, reputation systems, machine learning and advanced grid computing systems to parse through more than one billion pieces of content daily, searching for security threats. Every hour, it scans more than 40 million Web sites for malicious code and scans nearly ten million emails for unwanted content and malicious code. Using more than 50 million real-time data collecting systems, the Websense ThreatSeeker Network monitors and classifies Web, messaging, and data content—providing Websense with unparalleled visibility into the state of content on the Internet and email.

This report summarizes the significant findings of Websense researchers using the ThreatSeeker Network during the six-month period ending in December 2008.

Websense ThreatSeeker Network Research Highlights, Q3 – Q4 2008

Web Security

- 77 percent of Web sites with malicious code are legitimate sites that have been compromised.
- The number of malicious Web sites identified by Websense Security Labs from January first, 2008 through January first, 2009 has increased by 46 percent.
- 70 percent of the top 100 sites either hosted malicious content or contained a masked redirect to lure unsuspecting victims from legitimate sites to malicious sites. This represents a 16 percent increase over the last six-month period.

Messaging Security

- 84.5 percent of email messages were spam. This represents a 3 percent decrease over the last six months.
- 90.4 percent of all unwanted emails in circulation during this period contained links to spam sites or malicious Web sites. This represents almost a 6 percent increase in emails containing malicious links to compromised sites.
- Shopping remained the leading topic of spam (22 percent), followed closely by cosmetics (15 percent) and medical (14.5 percent). This remained consistent over the last six months. Pornography-related spam increased sharply by 94 percent, but still only represented 9 percent of all email spam.
- 6 percent of spam messages were phishing attacks, representing a 33 percent decrease over the last six months. This represents a change in tactics as spammers concentrated on data-stealing Trojan horses and DNS poisoning tactics to lure victims to malicious sites.

Data Security

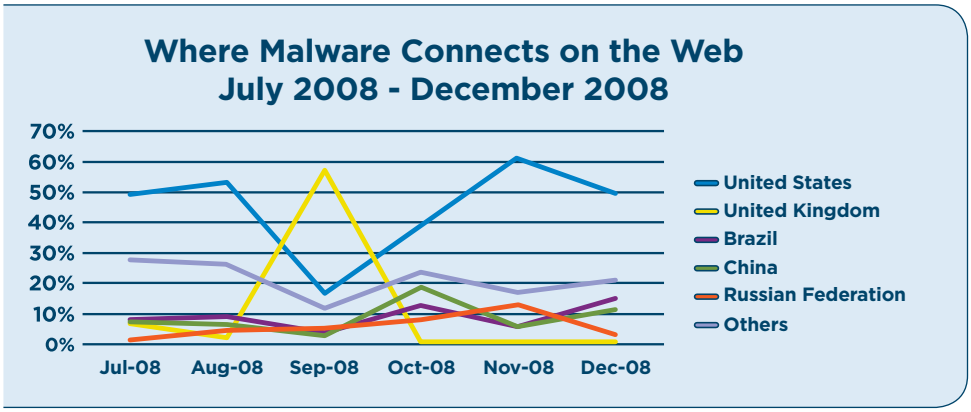
- 39 percent of malicious Web attacks included data-stealing code.
- 57 percent of data-stealing attacks are conducted over the Web. This represents a 24 percent increase over the six-month period.

With data-stealing Web and email attacks on the rise, Websense Security Labs is tracking where data is being sent around the globe.

Of the 57 Percent of Malware that Connects via the Web:

- 42 percent of malware connected to the U.S., down 27 percent over the last six-month period
- 16 percent of malware connected to United Kingdom
- 8 percent of malware connected to Brazil
- 8 percent of malware connected to China
- 5 percent of malware connected to Russian Federation
- 20 percent of malware connected to other countries

In the past six months and moving forward, Websense Security Labs expects to see less malware connecting to the United States as other countries' infrastructure improves and attackers start spreading their hosting locations around the world. This shift accounted for the spike in malware from the United Kingdom during September when a few pieces of malware caused a large number of connections to U.K. sites.



A Look Back at the Last Six Months

As expected, attackers capitalized on major events over the last six months. The Olympics, the 2008 U.S. presidential elections, and of course, the end-of-year holidays: Halloween, Thanksgiving and Christmas, provided fodder for both old and innovative attacks designed to steal personal or business information. Spammers continued to use malicious spam to invade blogs, search engines, forums, and Web sites to not only drive traffic to infected sites but also to increase search engine rankings in hopes of attaining more victims. But the most prevalent trend was the **continued use of Web 2.0 content to exploit weaknesses within the Web infrastructure** to attract the greatest number of victims. Search engines and social networking sites were the biggest targets over the last six months as hackers continued to get creative and leverage user-created content to compromise sites with good reputations.

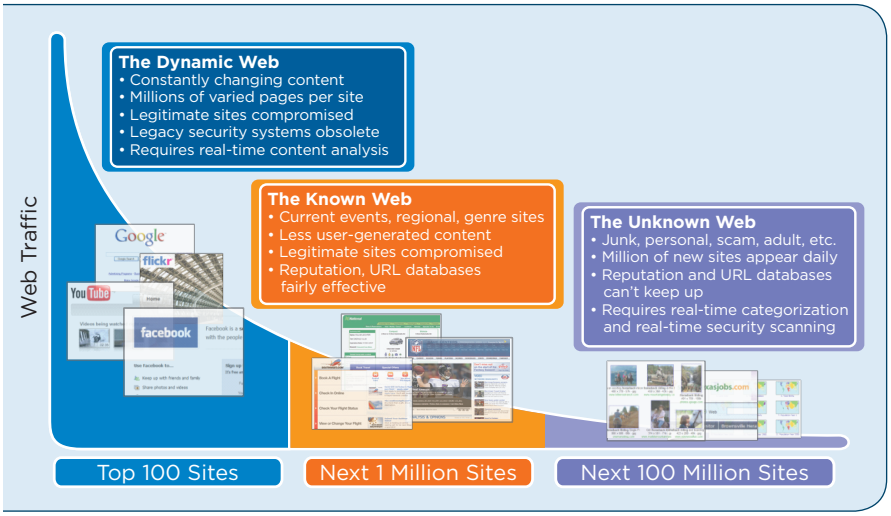
Changes in the Threat Webscape

Websense Security Labs classifies the Webscape into three general sections:

- The top 100 most visited Web properties tend to be classified as social networking or search sites such as search engines.
- The next 1,000,000 most visited sites, or the known Web, are primarily current events, regional and genre sites.
- Moving down the "long tail" of the Internet, or the unknown Web are junk, personal and scam sites, specifically set up for fraud and abuse.

Each area of the Webscape has its own unique security challenges, but the top 100 Web properties that encompass the largest amount of visitors is a growing target of attackers. Research shows that attackers continued to focus their attention on the Web 2.0 elements of the evolving Webscape, meaning that adaptive content classification and dynamic content scanning is now required to protect businesses and their information.

Not surprisingly, sites that allow user-generated content comprise the majority of the top 50 most active distributors of malicious content. Sites like mylivepage.com, blogspot.com and blogdrive.com all offer free hosting and good reputations to malware authors—the perfect combination to compromise unsuspecting users.



The top 100 most visited Web sites:

- Represent the majority of all Web page views, and are the most popular target for attackers. With their large user base, good reputations and support of Web 2.0 applications, these sites provide malicious code authors with abundant opportunity.
- Websense Security Labs identified that **90 percent of the top 100** sites are categorized as social networking or search. This remained static over the last six-month period.
- **More than 45 percent of these sites support user-generated content.** This remained consistent over the last six-month period.
- **70 percent of these sites either hosted malicious content or contained a masked redirect** to lure unsuspecting victims from legitimate sites to malicious sites. In many cases these redirects appeared as the actual Web site, when in fact the content served on that page was being hosted elsewhere. **This represents a 16 percent increase** over the last six-month period.

Business Growth Driving Web 2.0 Adoption in the Workplace

More and more organizations are beginning to embrace Web 2.0 technologies to facilitate collaboration across organizational and technology silos and to build new communication channels with customers, partners, and employees around the globe. Web 2.0 aims to enhance user creativity, information sharing, collaboration, and functionality of the Web. These features enable social networking, video sharing, blogs, Web publishing, plus other popular methods of information and content creation, editing, sharing, and distribution. However given the changing threat landscape, organizations need to be aware of the unique risks these sites pose to their essential information.

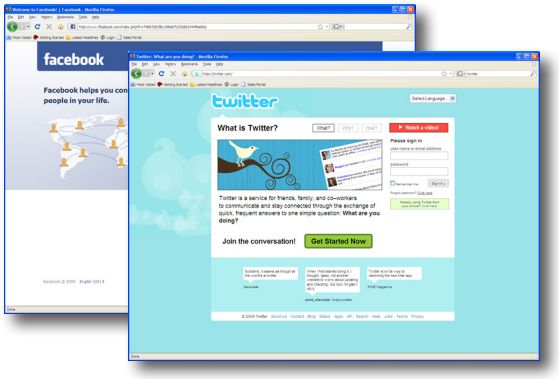
A new generation is driving Web 2.0 use in the workplace. The use of social networking sites like Facebook and MySpace are the "new email" and mode of communication, and the latest generation expects to be able to use their Web 2.0 devices and sites when they enter the workforce. In addition, marketing and communication departments are pushing IT departments to open up this access in an effort to grow and maintain their customer base.

Parallel Trends: The Increased Use of Web 2.0 Sites for Malicious Purposes

As Web 2.0 tools such as Twitter continue to make headway into corporations as a way to improve customer intimacy and branding, we see a parallel rise in Twitter being used for malicious purposes. Many organizations lack adequate security technologies and practices to enable safe Web 2.0 use to protect from data loss and malicious attacks. Spammers and malware authors are using this power to carry out various attacks.

The nature of Web 2.0 services, which allow users to create their own content, has provided attackers with more resources to carry out their malicious activities. Over the last six months a slew of security vulnerabilities have been found on Facebook, Twitter and Justin.tv.

Facebook continues to be plagued with outbreaks caused by a worm known as Koobface that propagates by sending notes to Facebook friends of someone whose PC has been infected. Attacks broke out in August but resurfaced again in November when malicious links, disguised as links to popular video clips, prompted users to download a malicious executable disguised as a codec that could steal confidential or sensitive information such as credit card numbers or intellectual property from the user's desktop. The potential losses in intellectual property ranged from reading of someone else's email, forcibly installing Facebook applications on one's profiles to spreading malicious links throughout the network.



Spammers continue to abuse Web 2.0 sites and have expanded their tactics beyond email. Instead of just using the typical obfuscated JavaScript redirect through sites like Blogspot, spammers are beginning to leverage the pervasiveness of Web 2.0 sites such as YouTube, Livefilestore, Picasa and Imageshack.

Security Trends

Blended Threats Deliver Major Hits on Brand-Name Reputations

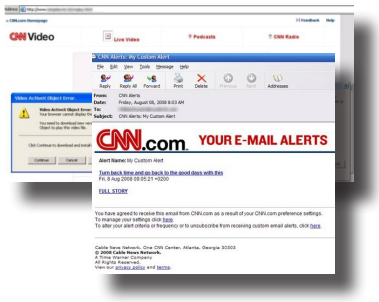
Continuing the trend identified by Websense during 2007 and the first half of 2008, attackers are taking advantage of flaws in traditional security measures to bypass reputation-based systems to increase attack effectiveness.

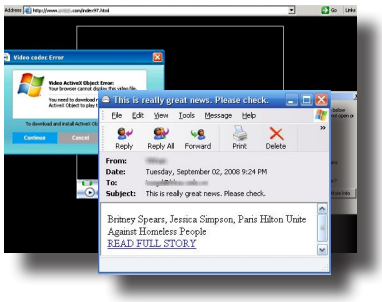
During the second half of 2008, the volume of legitimate Web sites compromised with malicious code continued to surpass the number of sites created by attackers specifically for malicious purposes. In the second half of 2008 **more than 77 percent of the Web sites Websense classified as malicious were actually sites with seemingly good reputations that had been compromised by attackers.** This represents a 2.5 percent increase over the last six months.

In August, Websense was the first to discover that CNET Networks, a media company owned by CBS Corporation, was compromised when malicious code implanted on its site infected unsuspecting visitors. In addition, highly visible sites like BusinessWeek.com, BillOreilly.com, and the New York Times faced serious Web attacks that unknowingly exploited unsuspecting visitors.

The convergence of Web and email threats—or blended threats—has **increased by 6 percent since June 2008.** Websense Security Labs reports that now more than **90 percent of all unwanted emails in circulation during this period contained links to spam sites or malicious Web sites.**

During the month of September alone, Websense Security Labs ThreatSeeker Network discovered huge volumes of spam wrapped up in CNN and MSNBC themed templates. These emails contain links to a trusted news page containing many legitimate links, but have been designed to encourage users to download a malicious application posing as a video. The emails entice users to download a video, which is actually a malicious file, by listing the top 10 stories or a wave of fake celebrity news covering popular stars including Britney Spears, Jessica Simpson and Paris Hilton.





Spam innovation

While phishing attacks decreased 33 percent over the last six months, spammers continued to innovate by switching tactics in order to increase infection success rates. Websense reported an increased use of data stealing Trojans and DNS poisoning tactics to lure victims to malicious sites.

Spammers continued to use everything in their arsenal, including different hostnames, page names, executable names and different templates in order to evade detection. Whether it was embedding a link directly to a malicious executable, or a Web page with a malicious template, or drive-by exploits linked from inside I Frames in the loaded pages, **spammers continued to change their campaigns in order to gain success.**

One of the most successful campaigns over the last six months that accounted for a high percentage of spam redirected victims to exploit-laden Web pages with pornographic videos, enticing them to install what really was a Trojan downloader. Generic streaming videos were subsequently used to lure victims to the path of infection. Spammers then shifted gears by quickly following up with the use of open redirects and celebrity photos, capitalizing on the world's fascination with Angelina Jolie, to encourage recipients to click malicious links.

Further driving innovation was the successful shutdown of two California-based hosting companies, McColo and Intercage/Atrivo, by upstream providers for hosting botnet command and control (C&C) servers as well as malicious code. Shutting down McColo in November had the effect of a 50 percent drop in all spam on the day it was closed, but spammers proved their resilience and rates subsequently recovered. Shutting down Intercage/Atrivo had a similar effect plus substantially stopped the Storm botnet from spreading. In the coming months it is likely that spammers will distribute their servers as well as move to foreign hosting providers to prevent similar shut-downs. Websense Security Labs will be tracking this trend in future reports.

Leaky Pipes Lead to Data Loss

2008 had fewer high-profile data leaks but maintained the same volume over 2006 and 2007. The downturn in the economy, cut-backs in personnel, the failure of corporations, and decreased security investments have created the perfect circumstances for significant data loss in 2009. According to Websense Security Labs, **57 percent of data-stealing attacks are conducted over the Web. This represents a 24 percent increase from July to December 2009.**

Organizations will be forced to do more with less, and their dogged determination to hit revenue targets will increase their tolerance to risk. If organizations fail to implement Web-based security to manage the traffic on their system, these types of attacks are likely to increase in 2009, causing more headaches for organizations across all industries.

Hotels often offer insufficient IT security, putting traveling employees at risk every time they stay at a U.S. hotel. But hotels aren't the only ones struggling; banks continue to be a popular target for rock phishers. Using their complex and fast-flux infrastructure, Rock Phishers have been successfully obtaining user account credentials over the last few months. Wachovia, Eastern Bank, Bank of America, Ocean Bank and Bank of the West were victims of these types of attacks. But perhaps the most surprising news was that universities continue to be the leading source of data leaks, ranking significantly higher than organizations in other industries including finance and retail.

Websense Security Labs Findings Include*:

- **Data loss from healthcare organizations rose by 126 percent in 2008 (over 2007)**
- **Data loss from insurance providers rose by 140 percent in 2008 (over 2007)**
- **Finance, technology, and manufacturing were the three industries with the greatest number of records lost (over 46 million records or 63 percent of all records lost in 2008)**
- **Retail showed a decline in the number of leaks and records lost, year-over-year, in part because of the massive amount of data loss they incurred in 2007 with such incidents as the TJX breach**
- **Federal government showed a marked increase in the number of data leaks in the second half (specifically Q3) of 2008. So too did city government**

The Web Remains the Number-One Attack Vector

Attackers continue to target free software downloads or file sharing sites with good reputations where users can upload or host content for free. **The number-one host of malicious files over the last six months was ironically, cleanmovie.net.** Evidently, it wasn't clean of malware. Cleanmovie.net accounted for almost eight percent of all malicious files hosted on the Web. Rounding out the top sites hosting malware between July 2008 and December was kit.net (three percent), variations of the URL myprivatetube (two percent), and archiveviewsoftware.com (two percent).

URLs remained a popular source of malicious code due to typo squatters, hackers hoping to exploit users that incorrectly entered a URL and landed on an imitation or fake site that looked very similar to the legitimate site. Of the top 50 sites hosting malicious code, variations of the popular social networking site classmates.com accounted for a large number of malicious files and pages on the Web over the last six months. Other typo-squatter victims included best-soft-for-pc.net and c-net-download.net.

The number-one host of data-stealing code over the last six-month period was kit.net, accounting for just about eight percent of all data stealing code on the Web. It was followed closely by more file sharing or free software download sites including again variations of myprivatetube.net at (six percent), sapo.pt, (three percent) livefilestore.com (two percent), and cleanmovie.net (one percent). Even Google pages, with its brand-name reputation, proved to be a dangerous site for users without the right Web security protection.

* Raw data above provided by Data Loss Open Security Foundation.

Top 10 Web Attack Vectors in Second Half of 2008:

As Internet users increase, the Web attack vector continues to grow. Web servers are increasingly compromised through persistent cross-site scripting (XSS) and SQL injection as well as DNS cache-poisoning attacks. The Web Application Security Consortium reports that 97 percent of sites it studied continue to be plagued with significant vulnerabilities.

Below are the top ten Web attack vectors over the last six months. Browser vulnerabilities, SQL injection attacks and the increase of social networking vulnerabilities rounded out the top three vectors. This list remains relatively consistent with the previous top-ten Web attack vector list cited during the first half of 2008.

1. **Browser vulnerabilities**
2. **Rogue antivirus/social engineering**
3. **SQL injection**
4. **Malicious Web 2.0 components (e.g. Facebook applications, third-party widgets and gadgets, banner ads)**
5. **Adobe Flash vulnerabilities**
6. **DNS Cache Poisoning and DNS Zone file hijacking**
7. **ActiveX vulnerabilities**
8. **RealPlayer vulnerabilities**
9. **Apple QuickTime vulnerabilities**
10. **Adobe Acrobat Reader PDF vulnerabilities**

Browser vulnerabilities continued to plague unsuspecting users. Opera version 9.5.1 enabled attackers to steal arbitrary samples of data in memory from desktops through specially crafted JavaScript code while vulnerabilities in Firefox provided attackers additional opportunities for spoofing by exploiting alternate names on self-signed certificates.

In August 2008, Digg, MSNBC, Newsweek, and MSN Norway were hit by a series of malicious third-party banner ads, which led visitors to rogue security software sites and hijacked the clipboards of visitors. One of the vulnerabilities exploited was an integer overflow in Adobe Flash (CVE-2007-0071). That same month, Websense Security Labs discovered that a major Chinese ISP, China Netcom (CNC), had its DNS cache poisoned. Unsuspecting customers were redirected to a malicious site when the hostname in a URL was mistyped.

Additional Metrics

Websense Security Labs tracks the following metrics to identify details about Web and email-based attacks against data and businesses.

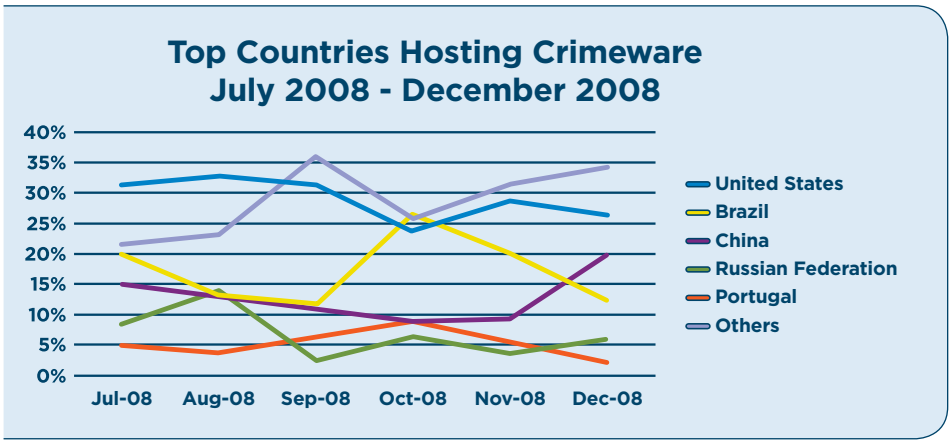
Gone Phishing: Top Countries Hosting Phishing Sites

Despite a decrease in phishing emails, Websense did see an increase in “money mule” and “work from home” scams designed to extract banking information from unsuspecting victims. These scams lured users by email to provide account information via a compromised site. The line graph below demonstrates the top countries hosting phishing sites by month, with the highest number of phishing attacks.

Flawed Security Sites: Top Countries Hosting Crimeware

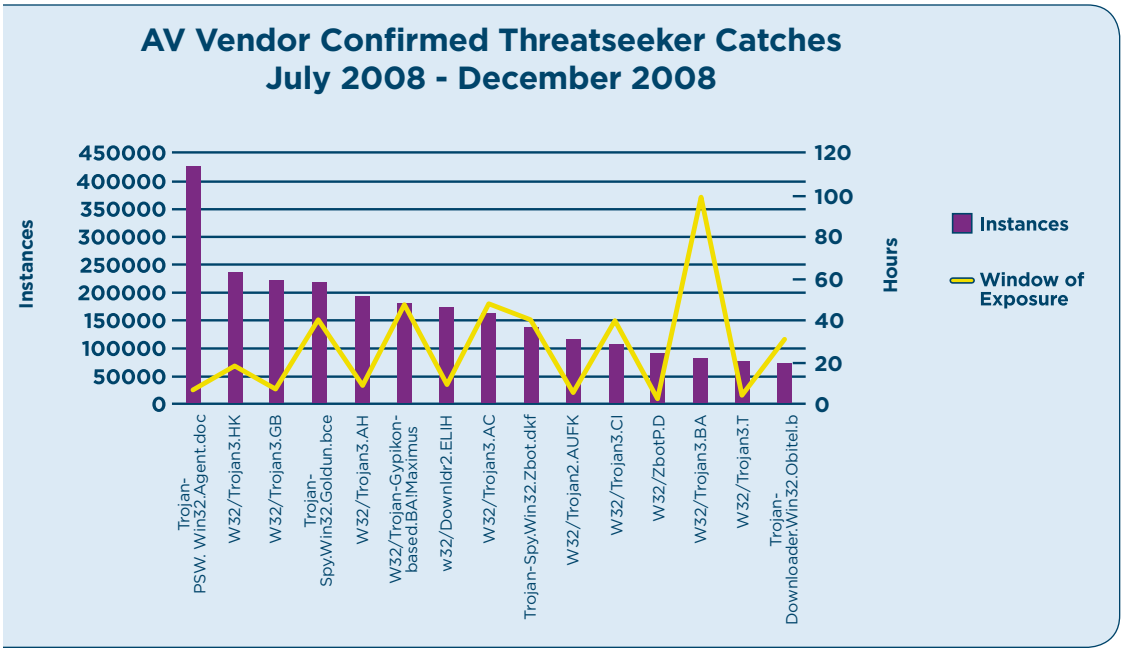
According to research published at the Symposium on Usable Privacy and Security meeting at Carnegie Mellon University on July 23-25, 2008, 75 percent of financial institution Web sites have at least one security flaw. In September 2008, financial institution ING's site was found to be susceptible to CSRF attacks, including one that could enable an attacker to transfer money out of a victim's account. Web threats also plagued Erste Bank, a large bank in Central Europe.

The line graph below demonstrates the top countries by month hosting crimeware, a class of malware designed specifically to automate financial crime. Over the last six months, the majority of malware was hosted in the United States and Brazil.



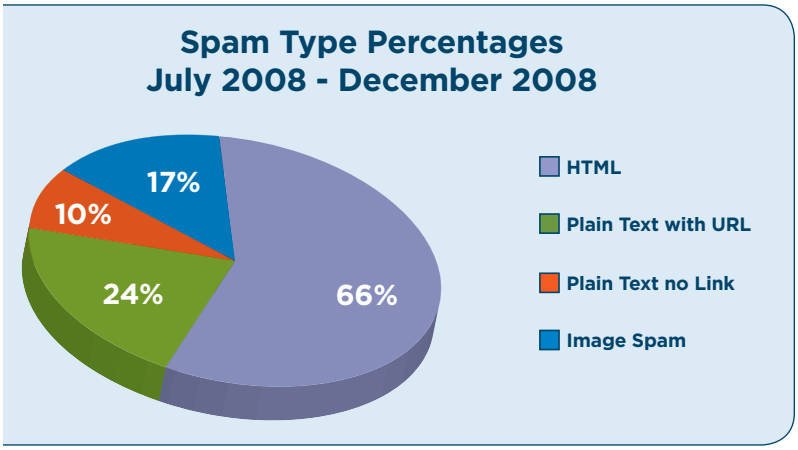
From Discovery to Patch: Window of Vulnerability

The ThreatSeeker Network discovers many malicious applications being circulated via email, drive-by downloads, exploit code, and other mechanisms employed by creative malware authors. Websense security supplements antivirus and firewalls by seeking out threats before customers are infected and provides protection within minutes of discovery—before patches and signatures are available. The chart below shows the window of exposure between threat detection by Websense ThreatSeeker Network and the release of the patch by antivirus software providers. The dates below represent the time it took for the antivirus vendors to publish a signature for the malicious threats Websense detected.

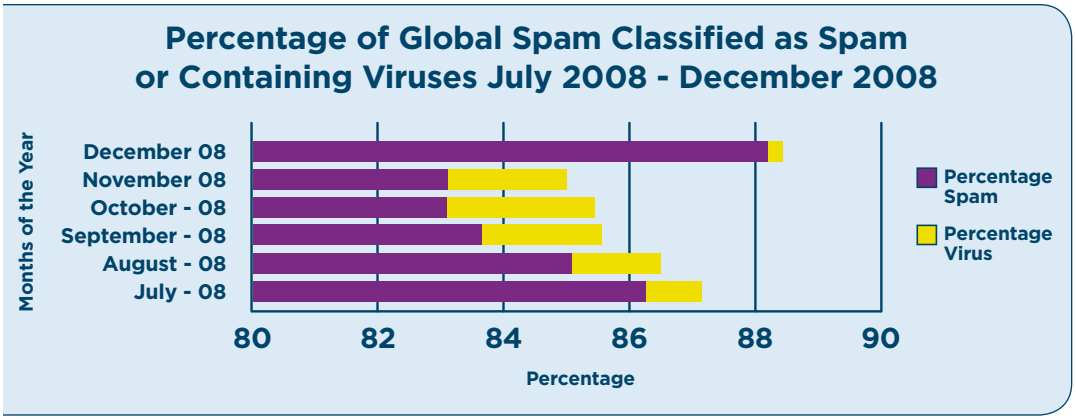


Spam Types

In the past six months Websense Security Labs has seen spammers continue to move away from image spam and towards the inclusion of links to spam Web content. This is also reflected by malware authors who opt to distribute malicious content via URLs rather than message attachments.

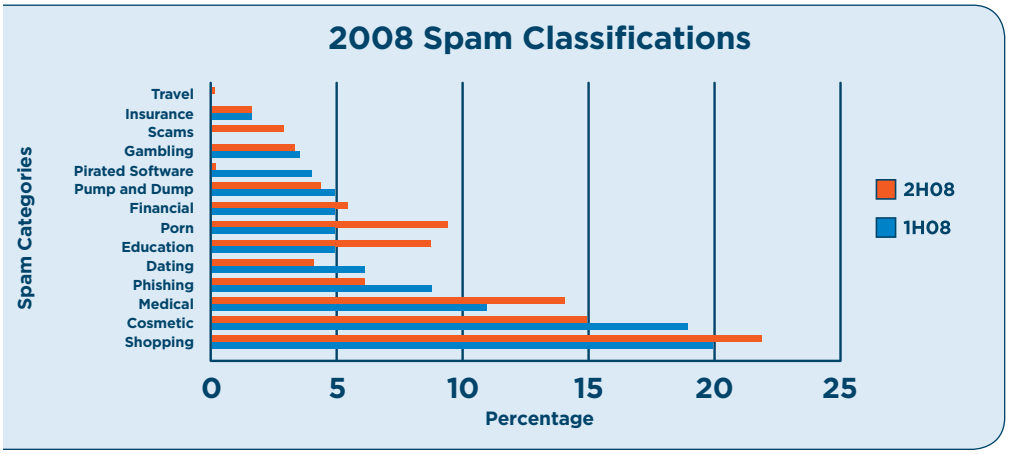


Over the last six months, the global number of messages containing viruses is low in comparison to the number of messages classified as spam. The percentage of email messages flagged as spam decreased by three percent over the last six months.



Over the last six months, the volume of pornographic spam increased 94 percent, but was still only the seventh most popular target for spammers. The three most popular topics for spam remained shopping (22 percent), cosmetics (15.1 percent) and medical (14.5 percent.) Despite an announcement from the Federal Trade Commission in October claiming a major shut down of a global spam network that advertised fraudulent drugs and accounted for one third of the world's spam, medical spam increased by 32 percent over the last six months. This implies that the spammers' mass-mailing underground economy is distributed, and posted a strong potential for future online marketing of their products.

Spammers continue to use social networking sites to learn more about their victims. This increased sophistication helps spammers become more targeted with their attacks and continues to help them increase their conversion rates. As shown in the bar chart below, Websense Security Labs classifies spam into the following 14 categories:



Websense Security Labs Firsts

Phishing the Beijing Olympics Lottery

Attack Date: 08/05/2008

Hackers capitalized on the summer Olympics by trying to trick users into buying tickets for the big event. Websense Security Labs ThreatSeeker Network discovered a rogue Beijing Olympics ticket-lottery Web site that used the hostname beij***2008.cn, a clear typo-squat to the official Olympic Games Web site at http://www.beijing2008.cn/. The social engineering tactic lured users into dialing a toll number to retrieve an access code for an available ticket. The toll number was likely an additional revenue generator for the scammers as callers would then be charged a premium rate for making that phone call.

Users who input the supplied access code were forwarded to a Web page designed to collect personal information, including credit card details, to pay a relatively small sum of RMB600 for the ticket (approximately $87 USD). This phishing Web site employed a phone-call verification step, garnering a higher level of trust from unsuspecting users. For more information on this alert click here.

CNET Networks Site Compromise

Attack Date: 08/06/2008

CNET Networks, a media company owned by CBS Corporation had one of its Web sites fall prey to attackers who planted malicious code on CNET's site aiming to infect visitors to the site. Websense was the first to discover this attack and promptly reported it to CNET for action. The malicious code was observed to exploit a known integer overflow vulnerability in Adobe Flash (CVE-2007-0071).For more details on this compromise, view the alert here.

US Presidential Malware–Barack Obama Interview Lure

Attack Date: 11/05/2008

The elections proved to be a successful topic for spammers over the last six months. In November, Websense ThreatSeeker Network discovered that malware authors were capitalizing on the announced results of the 2008 US presidential election. Malicious email lures were being sent, promising a video showing an interview with the advisors to the newly elected US president. Unsuspecting users who opened the email risked having malicious software installed designed to steal sensitive or personal information. For more details on this attack, view the alert here.

Mass Injection Attacks: Energy Conservation Systems Pty Ltd (ECS) Australia

Attack Date: 12/17/2008

Websense Security Labs ThreatSeeker Network discovered that an Energy Conservation Systems Pty Ltd (ECS) Australia courtesy site was infected with a mass JavaScript injection that delivered a malicious payload. Multiple pages on the site have been mass injected, attempting to deliver malicious payloads from 12 different hosts. Energy Conservation Systems Pty Ltd (ECS) is Australia's market leader in energy and water management for all market sectors: public, educational, industrial, commercial and large-scale residential. In an effort to protect their visitors, Websense Security Labs has contacted Energy Conservation Systems Pty Ltd (ECS) Australia to advise them of the threats on their site. Websense ThreatSeeker Network has been tracking how such attacks prevail over such reputed Web sites, targeting their peers, their own users, and other visitors. For more information view the alert here.

A Look Forward and Summary

As the stock market continues to falter and the world economy dips, the malware economy continues to thrive. Websense Security Labs predicts that in 2009 organizations will need to ensure risk mitigation keeps in step with the threat climate. Global enterprises must rethink their approaches to Web, data and messaging security. Instead of thinking about technologies, organizations must think of protecting their essential information, and especially their data, including:

- **WHO** is authorized to access Web sites, information or applications
- **WHAT** information is sensitive and must be protected
- **HOW** information can be exchanged
- **WHERE** information can be sent

The following are the top six predictions for 2009 that organizations should be planning for to ensure their essential information remains protected.

1. **The "cloud" will increasingly be used for malicious purposes**
   Cloud-based services, such as Amazon Web Services (AWS), Microsoft Azure, and GoGrid, provide businesses and users with easy-to-use, rent-as-you go opportunities for storage and large-scale computing at a low cost. But these services also are an attractive target for cybercriminals and spammers to exploit. Websense predicts that in 2009 we will see an increase in misuse of the cloud. The cloud may be used simply to send spam or to launch more sophisticated attacks, including hosting malicious code for downloads, uploading stats, and testing malicious code.

2. **An increased use of Rich Internet Applications (RIAs) like Flash and Google Gears for malicious purposes**
   There is growing adoption of browser-based Web applications that are either replacing or being used alongside traditional desktop applications. Examples include Web-based CRM systems, Google Docs and other Web-based office tools. Creating a rich Internet experience through a browser-based application is created with technology called rich Internet applications (RIA). With the explosion of demand for these applications, for developers who use RIA technologies such as Google Gears, Air, Flash and Silverlight to build large Web 2.0 Internet applications, security is an afterthought, opening up the door for cybercriminal abuse. With RIA popularity exploding, we predict that in 2009 we will see large scale attacks using both exploits found within the core RIA components as well as the user-created services that allow attackers to remotely execute code on user machines.

3. **Attackers take advantage of the programmable Web**
   The Web 2.0 world is one in which open Web APIs, mashups, gadgets etc. allow Web sites to share and use functionality from other Web sites. Web API's are being released at a record rate, leaving little time for testing, and requiring a level of trust between users. Websense believes that in 2009 there will be a rise in the malicious use of some Web service API's to exploit trust and steal user credentials and confidential information.

4. **A significant rise in Web spam and malicious posting of content into blogs, user-forums and social networks**
   The rise in the number and popularity of Web sites that allow user-generated content will lead to a significant rise in Web spam and malicious posting of content into blogs, user-forums, and social networks sites for search engine poisoning, spreading malicious lures, and duping users into fraud. Additionally, this threat will be augmented by several new Web attack toolkits that have emerged that allow attackers to discover sites that allow posts and/or have vulnerabilities. Additionally more BOT's will add HTTP post functionality into their capabilities.

5. **Attackers will move to a distributed model of controlling botnets and hosting malcode**
   This year we saw two California-based hosting companies McColo and Intercage/Atrivo shut down by upstream providers for hosting botnet command and control (C&C) servers as well as malicious code. Shutting down McColo had the effect of a 50 percent drop in all spam on the day it was shuttered. Shutting down Intercage/Atrivo had a similar effect plus substantially mitigated the "Storm" botnet from spreading. We predict that because these botnet groups have thus far depended on only a few providers to host their C&C servers, they will distribute their servers as well as move to foreign hosting providers, making it harder for upstream providers, the Internet community, and law enforcement to find and shut them down.

A continued siege against Web sites with good reputations

In 2009 we will see more than 80 percent of all malicious content hosted on sites with good reputations. We will see more big name Web site compromises and more compromises of Web sites in the Alexa top 100,000 most visited. This includes regional attacks on popular Web sites in select properties, popular sporting sites, news sites, and continued placement of IFrames and other malicious redirection code within them.

The information and predictions contained within this report are based on analysis of current attack trends, cybercriminal techniques, and threat intelligence gathered by researchers using the Websense ThreatSeeker Network.

About Websense

Websense, Inc. (NASDAQ: WBSN), a global leader in integrated Web, data and email security solutions, provides Essential Information Protection™ for more than 43 million employees at more than 50,000 organizations worldwide. Distributed through its global network of channel partners, Websense software and hosted security solutions help organizations block malicious code, prevent the loss of confidential information and enforce Internet use and security policies. For more information, visit http://www.websense.com/.

Websense Security Labs

Websense Security Labs is the security research arm of Websense, Inc. that discovers, investigates and reports on advanced Internet threats. Unlike other research labs, Websense has an unparalleled knowledge of malware and where it resides on the Web. This allows Websense to detect and block new threats that traditional security research methods miss, enabling organizations to protect sensitive content from theft, compromise, or inappropriate use. Recognized as a world leader in security research, Websense Security Labs publishes findings to hundreds of security partners, vendors and other organizations around the world and provides security metrics to the Anti-Phishing Working Group.

Websense Security Labs – a Pioneer in Emerging Threat Protection

- Unparalleled visibility and discovery on a massive scale
- Real-time adaptive ability to respond to trends and threats in a Web 2.0 world
- Powered by a unified world-class research team
- Many first discoveries, including the unpatched, high-risk Microsoft Excel vulnerability (March 2008)
- First to market with phishing protection
- First to market with drive-by and backchannel spyware protection
- First to market with bot network protection
- First to market with crimeware/keylogger protection

Security Alerts

Register with Websense Security Labs to receive FREE security warnings about malicious Internet events, including spyware, spam, phishing, pharming, and corrupted Web sites.
http://www.websense.com/securitylabs/alerts/

Blog Highlights

The Websense Security Labs blog delivers the most current information and breaking news about security research topics and advanced Internet threats. Websense Security Labs investigates and publishes information about outbreaks, new threats, and other relevant Web security topics to protect organizations from increasingly dangerous Internet threats. For more information, visit the blog:
http://www.websense.com/securitylabs/blog