WEBSENSE SECURITY LABS™

STATE OF INTERNET SECURITY

Q1 – Q2, 2008

websense®

ESSENTIAL INFORMATION PROTECTION™

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 June, 2008.

Websense ThreatSeeker Network Research Highlights, Q1 – Q2 2008

Web Security

- 75 percent of Web sites with malicious code are legitimate sites that have been compromised. This represents an almost 50 percent increase over the previous six-month period.
- 60 percent of the top 100 most popular Web sites [1] have either hosted or been involved in malicious activity in the first half of 2008.
- 12 percent of Web sites infected with malicious code were created using Web malware exploitation kits, a decrease of 33 percent since December 2007. Websense researchers believe this decrease may be attributed to attackers launching more customized attacks to avoid signature detection by security measures.

Messaging Security

- 87 percent of email messages are spam. This percentage remains the same as the second half of 2007.
- 76.5 percent of all emails in circulation contained links to spam sites and/or malicious Web sites. This represents an 18 percent increase over the previous six-month period.
- 85 percent of unwanted (spam or malicious) emails contain a link.
- Pornography-related spam decreased by more than 70 percent and is no longer the most popular topic for spam. Shopping (20 percent), Cosmetics (19 percent), and Medical (11 percent) represent the majority of today's spam.
- 9 percent of spam messages are phishing attacks, representing a 47 percent increase over the last six months.

Data Security

- 29 percent of malicious Web attacks included data-stealing code.
- 46 percent of data-stealing attacks are conducted over the Web.

[1] Source: Alexa (www.alexa.com) data on Web traffic for top 100 Web sites

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

Of the 46.37 percent of malware that connects via the Web:

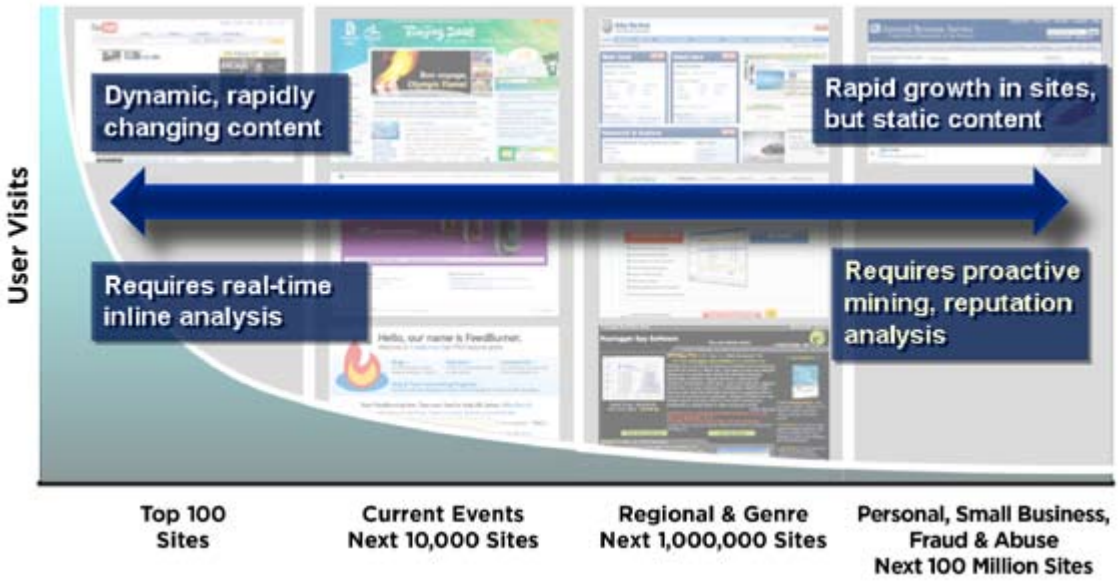
- 57.3 percent of malware connects to United States of America
- 6.19 percent of malware connects to China
- 5.5 percent of malware connects to Canada
- 4.27 percent of malware connects to Russia
- 4.11 percent of malware connects to Brazil
- 22.63 percent of malware connects to other countries

Cybercriminals Increase Attacks on Web Sites with "Good" Reputations

During the first 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 first half of 2008 **more than 75 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 50 percent increase over the last six months.

The Webscape Demonstrates Web 2.0 Sites Are a Fresh Target

Websense Security Labs classifies the Webscape into four 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 10,000 most visited sites are primarily current event and news sites and, down the "long tail" of the Internet, Web sites that are more regional and genre-focused. The growing tail end of the Webscape is comprised of personal sites like blogs, small business sites, and Web 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 continue 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. Below is a graphic of the Websense view of the Webscape:



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.
- More than 45 percent of these sites support user-generated content.
- 60 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 appear as the actual Web site, when in fact the content served on that page is being hosted elsewhere.

Security Trends

Tarnished Reputations

Continuing the trend identified by Websense in 2007, attackers continued to take advantage of flaws in traditional security measures and bypass reputation-based systems to increase attack effectiveness.

In April of 2008, Websense Security Labs discovered massive attacks that compromised hundreds of thousands of legitimate Web sites with good reputations worldwide with data-stealing malicious code. This attack included sites from MSNBC, ZDNet, Wired, the United Nations, a large UK government site, and more. In this attack, when a user's browser opened one of the thousands of compromised sites, a carefully crafted iframe HTML tag redirected users to a malicious site rife with exploits. As a result, malicious code, designed to steal confidential information, was launched on vulnerable machines.

In addition to Web exploits, email spammers are also taking advantage of the reputation of popular email services like Yahoo! and Gmail to bypass antispam systems. **During the first half of 2008, Websense Security Labs found spammers using sophisticated tools and bots to break the "CAPTCHA -" systems that were developed to keep email and other services safe from spammers and other malicious activity.** Microsoft Live Mail, Google's popular Gmail service and Yahoo! mail services were all compromised by this breakthrough method. Subsequently, spammers have been able to sign up for the free email accounts on a mass basis and send out spam from email accounts with good reputations. With a free sign-up process, access to a wide portfolio of services and domains that are unlikely to be blacklisted given their reputation, spammers have been able to launch attacks on millions of users worldwide while maintaining anonymity.

Attackers Are Changing the Game with Web 2.0

As more organizations and their employees are adopting Web 2.0 technologies for legitimate business reasons, users are given privileges such as directly editing Web content or uploading files—potentially causing more security issues as many organizations lack the adequate security technologies and practices to enable safe Web 2.0 use. The increase in Web 2.0 applications has allowed hackers to target users and businesses using mash-ups, unattended code injection, and other tactics providing yet another level of complexity for organizations and users that want to prevent data loss and malicious attacks.

Websense has found that the content of a single Web page may be comprised from multiple locations including a variety of disparate sources. The danger is that users typically associate the content they are viewing from the URL in the address bar, not the actual content source. The URL is no longer an accurate representation of the source content from the Web page. As such, organizations that enable their employees to view Web 2.0 technologies like iGoogle Web portals or social networking sites, wikis, and blogs, need real-time Web security protection to protect their employees and their essential information.

[2] CAPTCHA Definition: Completely Automated Public Turing test to tell Computers and Humans Apart

Malware masquerading as Web ads proved to be a popular means for hackers to distribute malicious content onto high-profile sites during the first half of the year. Websense Security Labs identified several instances where malicious banners ran on high-traffic, high-reputation sites such as MySpace, Excite.com, Yahoo! Mail and Perl.com to increase chances of exploiting a larger audience. MySpace unknowingly ran banners that pushed nefarious malware to unsuspecting users. With Excite.com, attackers used the notion of "transitive trust" to exploit the faith the user placed with the Web site. Trusting users didn't realize that the executable they were downloading came from embedded, malicious banners, and not from Excite.com. Antivirus vendors failed to identify many of these attacks.

The Web Remains the Number One Attack Vector

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. In June of 2008, Websense Security Labs received reports that the official Web sites of ICANN and IANA Domains were hijacked by a Turkish group called "NetDevilz" using DNS cache poisoning.

Over the last six months, Websense Security Labs has tracked hackers using toolkits to search for Web sites vulnerable to SQL injection attacks. Attackers target hosts with both a high profile and strong reputation, to maximize the number of visitors once the site has been compromised. In addition, client-based threats have increased with popular Web 2.0 components such as Facebook's "Secret Crush" application, which is actually ad-serving software, as well as multi-media applications that contain exploits such as Quicktime and Flash. Below are the top ten Web attack vectors over the last six months.

Top 10 Web Attack Vectors in 1st Half of 2008:

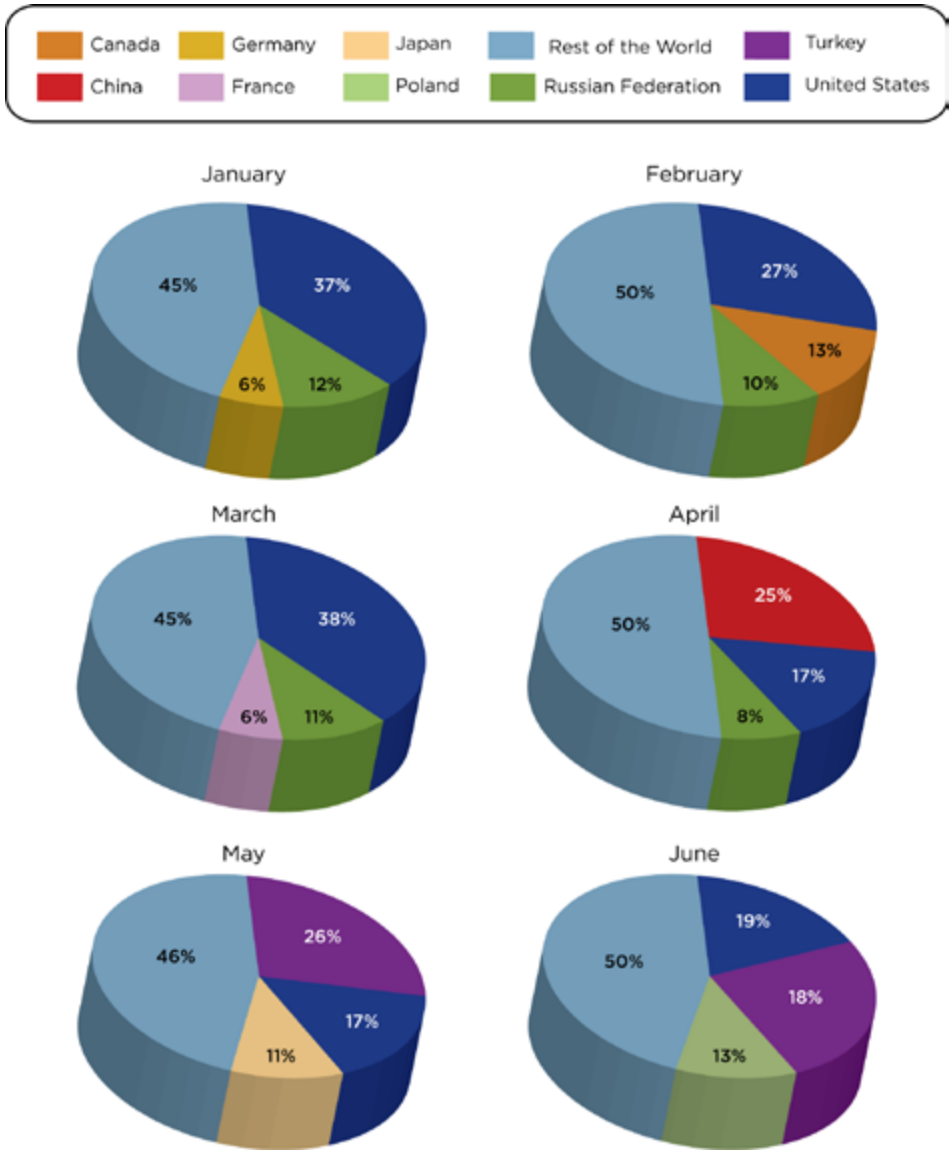
1. Browser vulnerabilities
2. Adobe Flash vulnerabilities
3. ActiveX vulnerabilities
4. SQL injection
5. Adobe Acrobat Reader vulnerabilities
6. Content management systems (CMS) vulnerabilities
7. Apple QuickTime vulnerabilities
8. Malicious Web 2.0 components (e.g. facebook applications, third-party widgets/gadgets, banner ads etc)
9. RealPlayer vulnerabilities
10. DNS cache poisoning

Metrics

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

Top Countries Hosting Phishing Sites (Jan 08 – Jun 08)

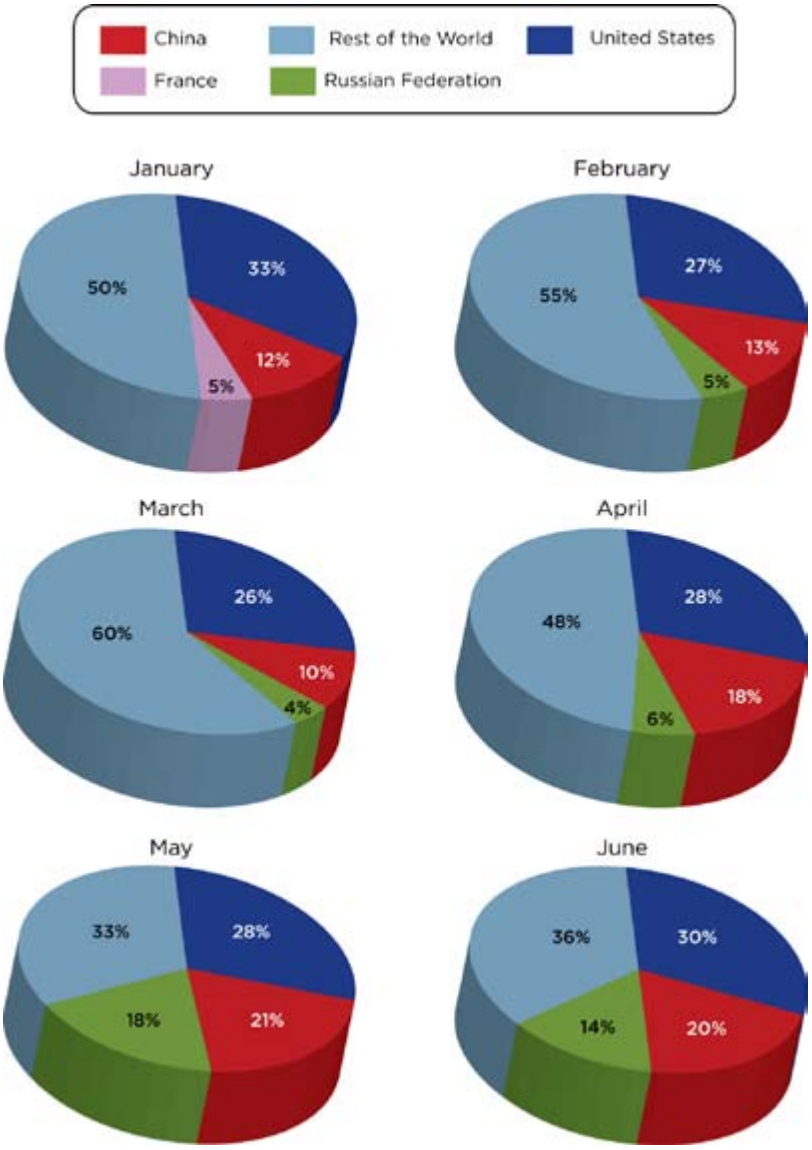
The pie graphs below demonstrate the top three countries, by month, with the highest number of phishing attacks.



Phishing attacks have been trending down over the last six months; this is in contrast to the same six months a year ago.

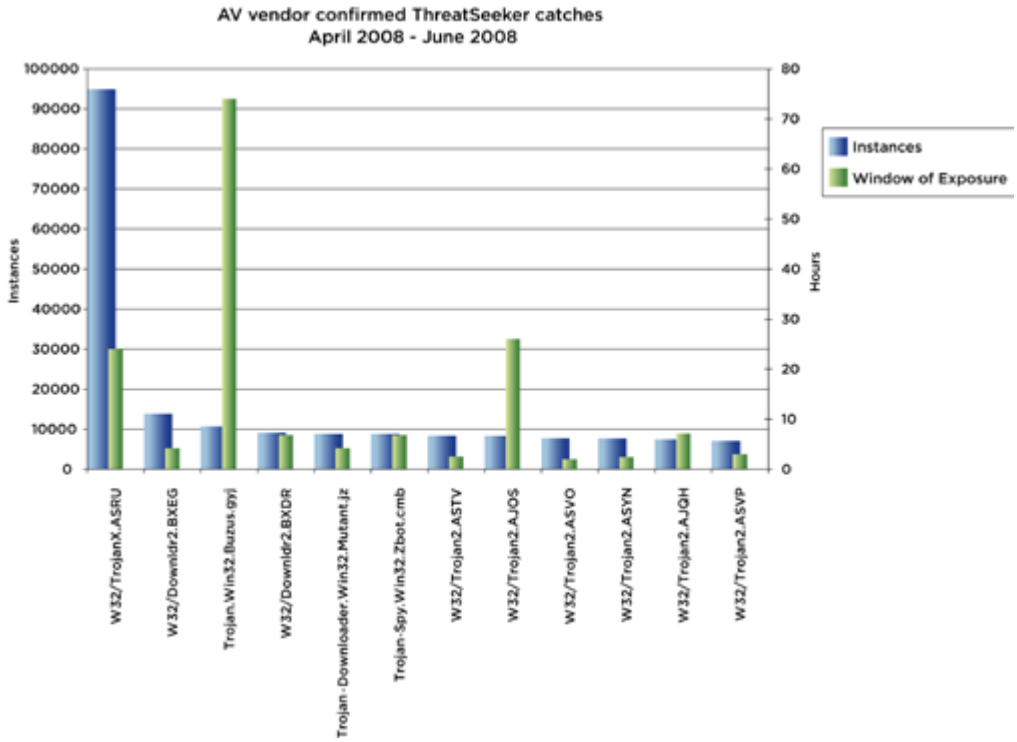
Top Countries Hosting Crimeware (Jan 08 – June 08)

The pie graphs below demonstrate the top 3 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 China.



From Discovery to Patch: Window of Vulnerability

Websense security supplements outdated 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.



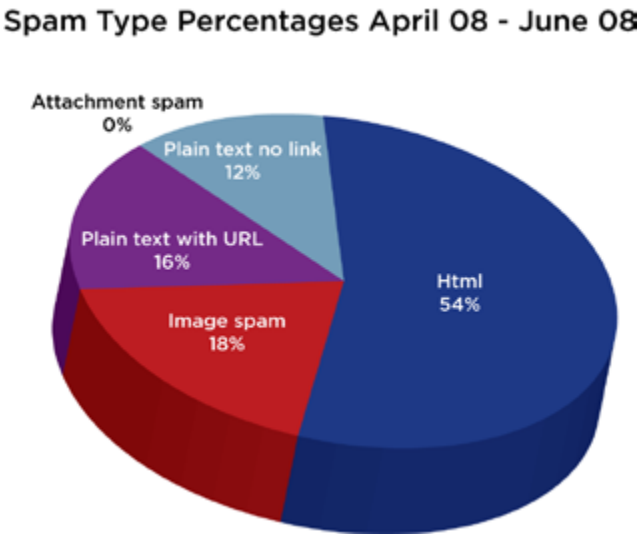
Blended Threats

The convergence of Web and email threats—or "blended threats"—continues to increase. Websense Security Labs reports that now more than 76.5 percent of all emails in circulation during this period contained links to spam sites and/or malicious Web sites. This represents a substantial 18 percent increase since December 2007.

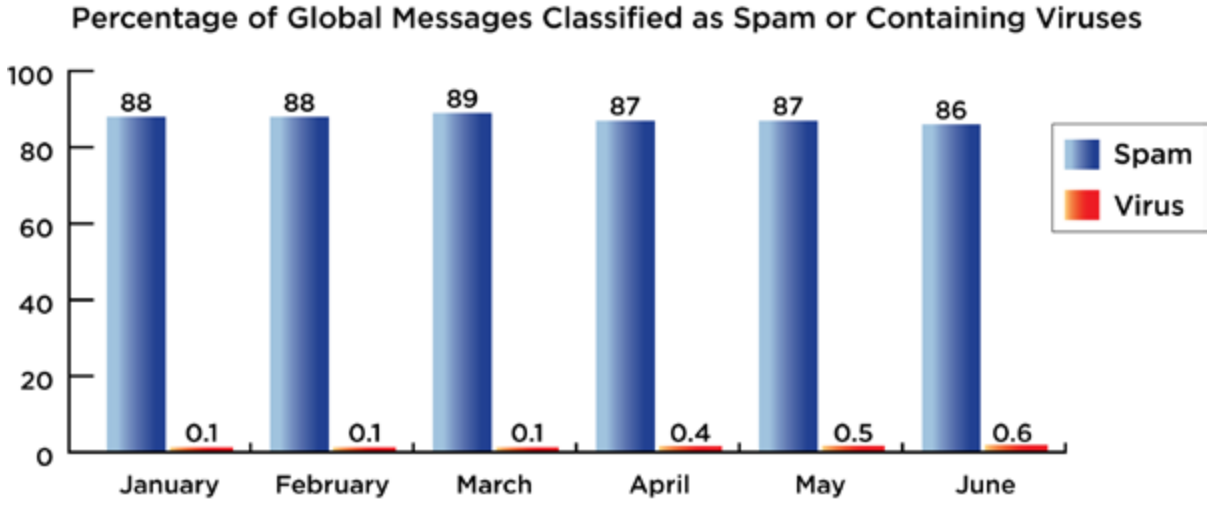
Examples of blended threats are the ***"Storm" attacks.*** The Storm attack authors have launched some of the most prolific attacks of the last few years. Storm is a perfect example of a blended threat that uses multiple attack vectors including DDoS, Web, Peer-to-Peer (P2P), encryption, and malware distribution. Websense Security Labs has been tracing the Storm worm since early 2007 when the first wave of the Storm worm erupted in the wild. Antivirus vendors have struggled to keep up with this widespread attack. Storm lures are presented as short, simple emails, enticing the victim to click preferred links and download a malicious file. Lures range from holidays like the Fourth of July, natural disasters like the earthquakes in China and most recently, popular events like the Olympics. These targeted spam campaigns represent one of largest professional botnets in the Internet's history. Storm's use of advanced polymorphism (or constantly changing attributes) makes it difficult for traditional security technology to detect.

Spam Types

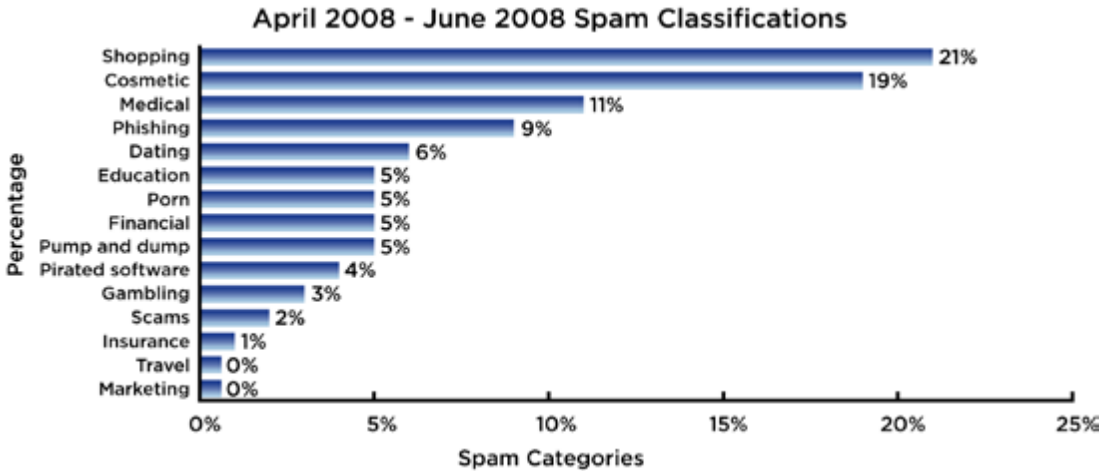
In the past six months Websense Security Labs has seen spammers move away from distributing spam through attachments, preferring instead to distribute URLs to spam-hosting and distribution sites. Additionally, Websense noticed **a reduction in image spam from 32 percent in December of 2007 to 18 percent in June 2008.**



Over the last six months, the global number of messages containing viruses is low in comparison to the number of messages classified as spam. However, the virus activity is steadily increasing, representing a 500 percent increase since December of 2007. The percentage of email messages flagged as spam remains static at 87 percent with a zero-percent change over the last six months.



Over the last six-months, the volume of pornographic spam, decreased more than 70 percent while shopping increased by almost 80 percent. The reason for the swap may be related to the fact that spammers are getting more sophisticated. They are using social networking sites to learn more about their victims and using targeted campaigns to increase their attack conversion rates. The three most popular topics for spam are now shopping (20 percent), cosmetics (19 percent) and medical (11 percent.) As shown in bar chart below, Websense Security Labs classifies spam into the following 15 categories:



Websense Security Labs Firsts

The following list highlights a few of the major attacks successfully identified by Websense Security Labs during the first half of 2008.

Spammers streamline anti-CAPTCHA operations on Microsoft Windows Live Mail and Gmail Attack Date: 02/06/08

Attack Details:
Websense Security Labs, with its ThreatSeeker Network, discovered that Windows Live Mail accounts, a free Web mail service from Microsoft, was being targeted by spammers using a new sophisticated technique to create thousands of Windows Live email addresses by cracking the CAPTCHA protection designed to prevent the creation of fraudulent accounts. Using a bot network, spammers established a connection to the registration page of the Microsoft-owned mail service and were able to bypass the CAPTCHA requirement 35 percent of the time. Free email services from Microsoft, Yahoo! and Google are rarely blocked by anti-spam filters, making accounts from these services highly profitable and valued by spammers. In addition, Websense Security Labs discovered that Google's popular Web mail service, Gmail, was being targeted by Spammers to create bots that are capable of signing up and creating random Gmail accounts for nefarious purposes. Websense researchers believe that the same group is involved in breaking the Microsoft Windows Live Mail CAPTCHA break as well as the Gmail CAPTCHA break.

Websense Security Labs researchers believe there are four main advantages to this approach:

- Signing up for an account with Google or Microsoft allows access to its wide portfolio of services.
- Google or Microsoft's domains are unlikely to be blacklisted by anti-spam filters.
- These services are free.
- It's difficult to identify illegitimate accounts as millions of users worldwide are using various Google services on a regular basis. This provides spammers with a layer of anonymity, making it harder to detect and track their actions.

Economic Stimulus Phish
Attack Date: 05/16/2008 Threat

Attack Details:
Eager recipients of the Internal Revenue Service economic-stimulus checks were taken for more than they bargained for with a phishing scheme. Websense Security Labs with its ThreatSeeker Network discovered a phishing attack that aimed to steal tax-payer's sensitive information, dubbed the "Economic Stimulus Phish". The attackers sent out an email to potential victims that provided a quick explanation of the recent economic-stimulus package and encouraged them to sign up for direct deposit by clicking on a link before May 17. It warned that if the recipient didn't respond in time, their refund would be delayed. Users that unsuspectingly clicked on the "Tax Refund Online Form" were asked for personal information such as their name, address, credit card, ATM pin number, bank name, and social security number.

Websense first to discover and protect against Microsoft Excel vulnerability
Published March, 2008 (Identified in November 2007)

Vulnerability Details:
Websense Security Labs with its ThreatSeeker Network discovered an un-patched, high-risk vulnerability (Cert# MS08-014) in Microsoft Excel in November 2007. Microsoft recognized Websense for the find in March 2008 when a patch was issued. The vulnerability allowed code execution within an Excel document without the knowledge of the user. Websense vigilantly watches for exploits of this vulnerability to protect organizations and their essential information from unnecessary threats. Websense will automatically block malicious code before it can infect an organization's computers.

A Look Forward & Summary

During the first half of 2008 as predicted, the number of compromised Web sites continued to grow and surpass the number of created malicious sites. Websense researchers expect this trend to continue as hackers become more sophisticated and continue to leverage the "good" reputations of Web sites to evade traditional security measures.

Websense researchers believe organizations should prepare for continuing challenges in during the second half of 2008 and encourages security managers to shift their protection emphasis from guarding against inbound attacks at the infrastructure level—a model suited to perimeter boundaries and the Internet as a simple content resource—to guarding essential information against blended threats and accidental or malicious loss, in tune with Web 2.0 and the Internet as a business platform.

Hackers will continue to get creative and leverage user-created content and Web 2.0 applications to create even bigger security concerns for organizations. Researchers expect attackers to see a rise in special interest attacks – targeting specific groups of people based on interests and profiles. With an increase in spam and "talk back" sections of new sites, new active media, Web modules, scripting and social networks, organizations will need to ensure their Web, messaging and data security programs are adequate to plug the holes and curb the new avenues hackers exploit to spread malicious code for financial gain.

To ensure risk mitigation keeps in step with the threat climate, enterprises must rethink their approaches to Web, messaging, and data security. Instead of thinking about technologies, organizations must think about data. How is it used? Who is using it? Where and when is it safe to use? Who can receive it? Which channels can safely send it?

A silo-based approach to e-mail and Web filtering will not provide the necessary protection against blended threats. Organizations should move toward comprehensive data-centric security that includes not only Web and messaging Security, but also data security to prevent information loss across all channels.

This data-centric view means that, rather than investing in protection silos with limited coverage, enterprises will mesh defenses across technologies, communication channels, and applications focused on protecting data. This integration increases the accuracy of detection and the quality of response. More than just proactive enforcement, this integration provides appropriate protection, because it allows the use of context to understand legitimate business uses and adapt responses. By protecting sensitive data, the essential information of each business, organizations can both embrace and defend the Internet business platform.

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

About Websense

Websense, Inc. (NASDAQ: WBSN), a global leader in integrated Web, messaging and data protection technologies, provides Essential Information Protection™ for more than 42 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.

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 today's 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, check out our blog:
http://www.websense.com/securitylabs/blog