



Research Highlights: Q3-Q4 2007



Websense® Security Labs™

Websense Security Labs, the security research division of Websense, discovers, investigates, and reports on advanced Internet threats that traditional security research methods miss. Recognized as a world leader in security research, Websense Security Labs publishes findings to hundreds of security partners, vendors, media outlets, military, and other organizations around the world 24 hours a day, seven days a week. With a team of global threat experts and operations in the Americas, Europe, Middle East, Africa and Asia Pacific, Websense Security Labs provides continuous monitoring of all Internet threats including Internet-borne threats, stemming from Web, email, instant messaging, and peer-to-peer file-sharing.

Key Findings

This report summarizes the significant findings of Websense Security Labs during the third and fourth quarters of 2007. The report includes a summary of key trends, security metrics, and stand-out attacks during the second half of the year, as well as the top ten security threat predictions for 2008.

The Attacks Storm In

The second half of 2007 was a microcosm of the ever-evolving security landscape.

The Storm attacks are some of the most active and prolific attacks of the last few years. This orchestrated attack is a combination of a worm, a Trojan horse, a bot, and a spam agent all blended into one. Since Storm uses multiple attack vectors including DNS, Web, P2P, encryption, and several evasion techniques, it is difficult to take down.

So called “Storm” attacks were launched in January 2007 as emails with an enticing subject line about a recent natural disaster. Over time they have evolved to use subject lines of interesting world events, either real or contrived. The attacks spread en masse during July with an Independence Day lure. The attacks continued to spread and plague security departments through the end of 2007 with several Christmas and New Year’s Day lures.

The Storm attacks were all well planned, resilient, and difficult for firewalls and signature-based technologies like antivirus to prevent. As a result, the attacks infected millions of machines worldwide, exposing millions of users and organizations without adequate protection. This attack clearly demonstrates the need to deploy sophisticated countermeasures to mitigate risk and protect against malicious threats.

Websense continues to prevent the infections of Storm attacks every day by blocking the IP address or URL of the master servers, rather than by blocking the IP of the proxy/bot that is redirecting the traffic or by blocking the malicious file download. For more information on how Websense protects against Storm attacks visit: <http://www.Websense.com/securitylabs/blog/blog.php?BlogID=141>

Tarnishing a Good Reputation

During the second half of 2007, Web attacks continued to increase and evolve as more and more legitimate Web sites were compromised by attackers. For the first time, the number of legitimate Web sites compromised with malicious code has surpassed the number of sites created by attackers. Today 51% of the sites Websense Security Labs classified as malicious are compromised Web sites, meaning they were not intentionally built for malicious intent. These sites pose a significant risk because many security companies rely on Web site reputation to protect customers. Compromised sites have a good reputation, plus they have a built-in group of visitors to the site. This raises the effectiveness of the attacks and diminishes the need for the attackers to create lures to get traffic to the sites.

Toolkits Come in Handy for Hackers

More than 18% of all malicious Web sites were created or compromised using professional toolkits widely available online. This represents a 3% increase from 2006.

Web 2.0 Attacks Increasing

By examining current attack trends, Websense Security Labs finds cybercriminal techniques are quickly evolving to not only evade detection but also to steal data and manipulate trusted content such as Web sites and applications. The increase in Web 2.0 applications, such as social networking sites, wikis, and blogs, facilitate collaboration and sharing between users. However, the increased popularity of these applications has driven hackers to target users and businesses using these emerging tools. Using mash-ups, unattended code injection, and other tactics, Web 2.0 hackers provide yet another level of complexity for customers that want to prevent data loss and malicious attacks.

Websense ThreatSeeker™ Technology

In development for more than five years within Websense Security Labs and based on more than ten years of experience classifying the Web, ThreatSeeker™ technology scans more than 600 million Web sites per week searching for malicious code. Along with Websense Hosted Web Security and Websense Hosted Email Security, which scan more than 350 million emails per week looking for email security threats, ThreatSeeker technology is the foundational technology behind the Websense Web security portfolio of solutions. Websense Global Threat Experts used ThreatSeeker technology to gather the security intelligence for all of the threats identified in this report.

ThreatSeeker Technology Q3-Q4 2007 Results*

- 51% of Web sites with malicious code are legitimate sites that have been compromised, rather than sites specifically commissioned by hackers
- 18% of malicious Web sites were created using a toolkit
- 87% of email messages are spam
- 65% of unwanted messages contain malicious URLs (including links to spam and malicious sites)

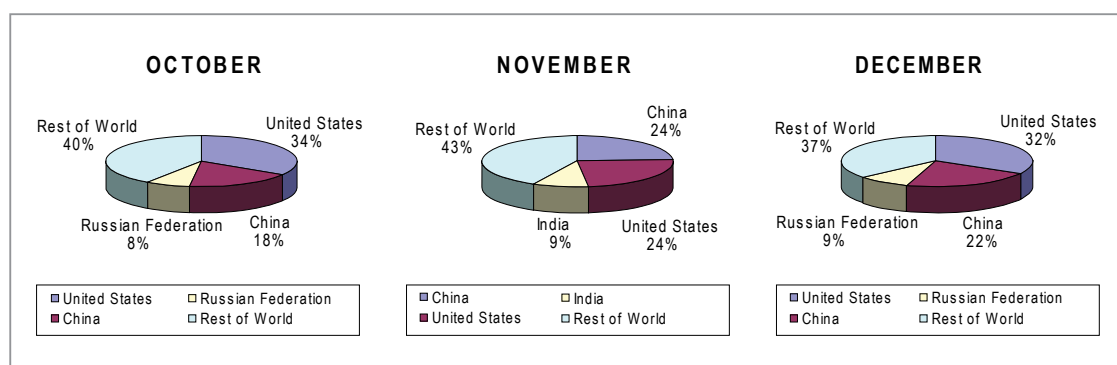
* The information contained within this report represents a small portion of the research activity conducted by Websense Security Labs during the second half of 2007.

Metrics

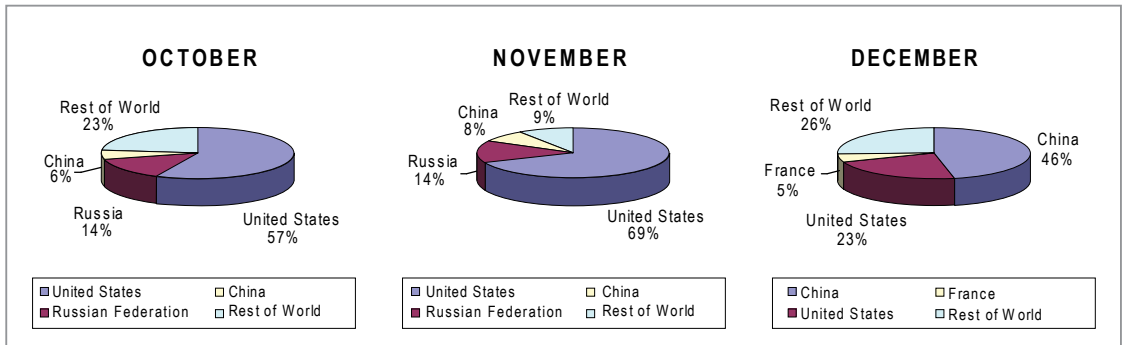
Websense Security Labs tracks the following metrics in order to identify details about Web and email-based attacks.

The following charts show that the United States, China, and Russia are the top countries hosting phishing and crimeware sites.

Top Countries Hosting Phishing Sites



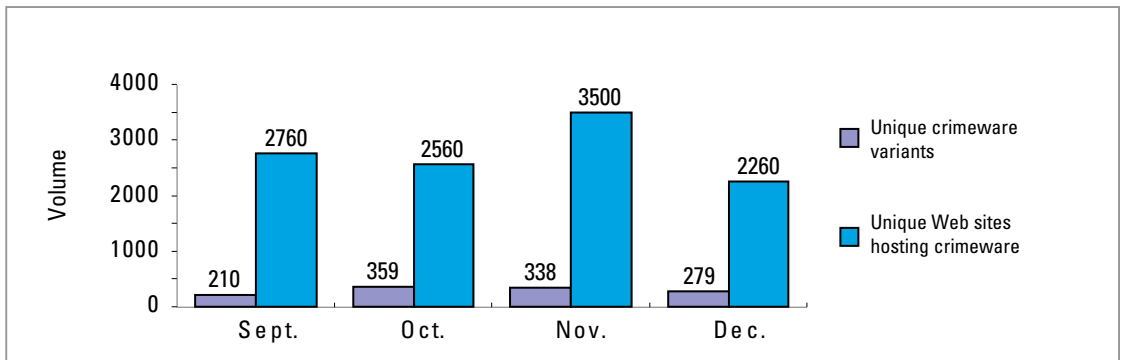
Top Countries Hosting Crimeware



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.

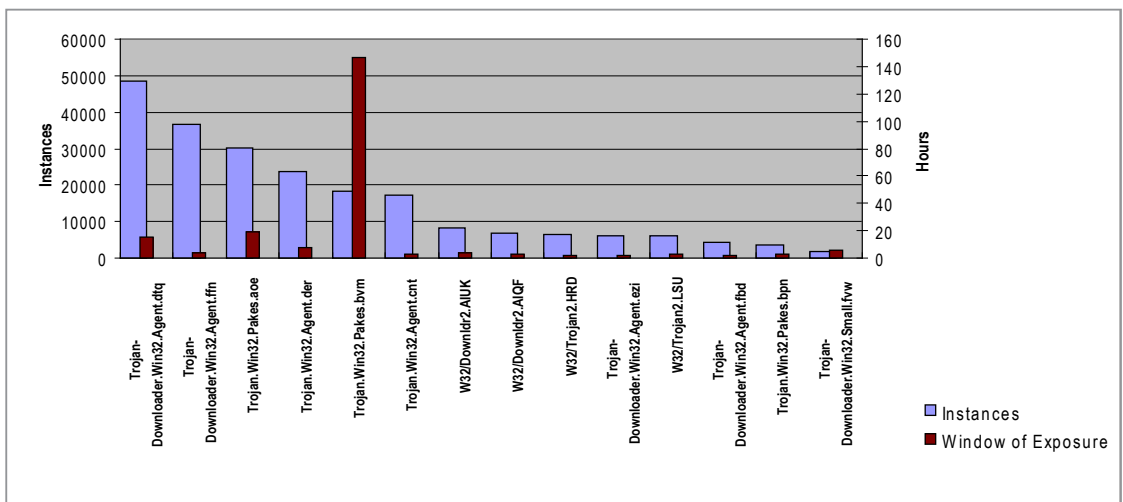
Changes in unique crimeware, a class of malware designed specifically to automate financial crime, remained relatively flat in Q4 while unique Web sites hosting malicious code spiked in November to represent a modest 13% averaged increase from the end of Q2.

Unique Crimeware Variants and Unique Web Sites Hosting Crimeware



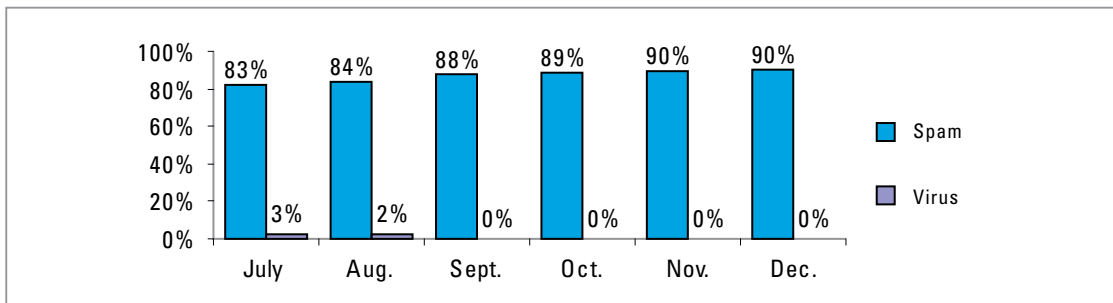
Websense security complements antivirus and firewalls by seeking out threats before customers are infected, protecting before patches and signatures are available, and providing accurate protection within minutes of discovery. As demonstrated in the chart below, Websense reduces the window of exposure for customers and provides protection for security customers before leading antivirus software providers.

Q4 AV Vendor Confirmed ThreatSeeker Technology Catches



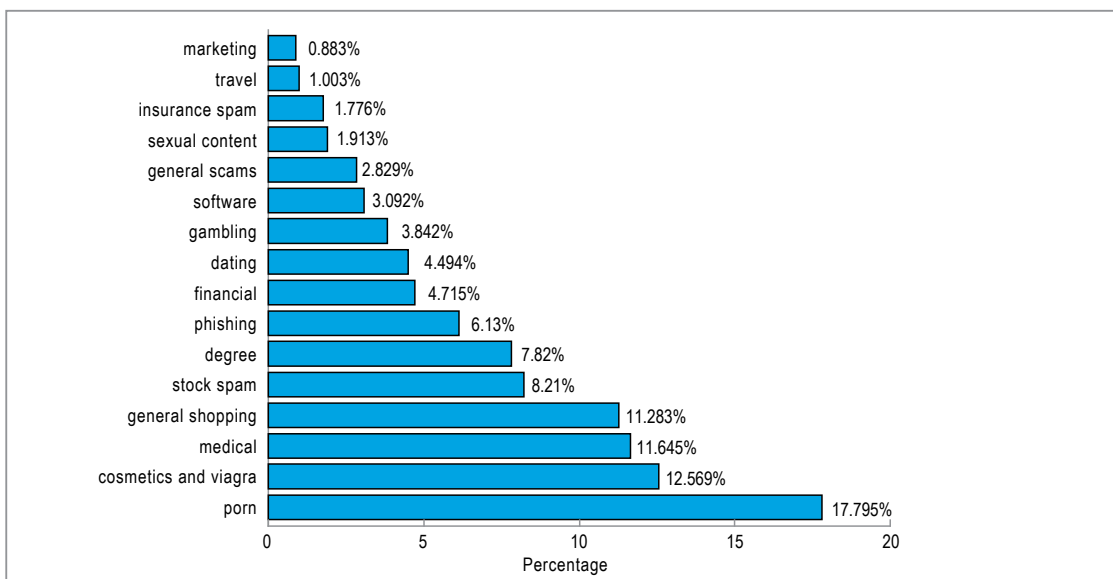
The global number of messages containing viruses is low in comparison to the number of messages classified as spam over the last six months. Changes remain relatively flat for both, as seen in the following chart.

Q3-Q4 Percentage of Global Messages Classified as Spam or Containing Viruses



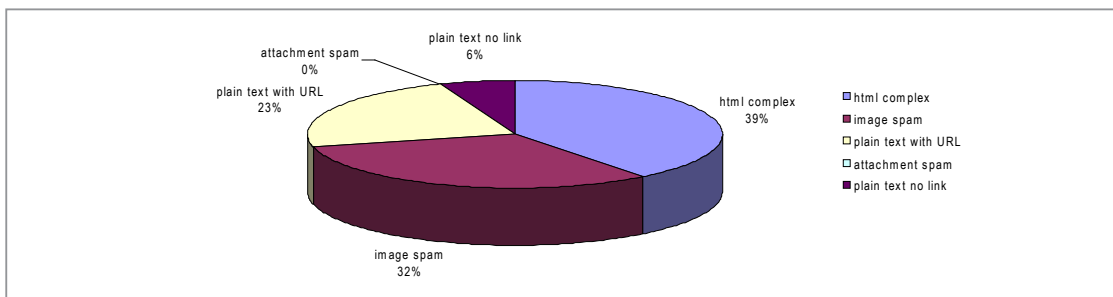
Over the last six months, the volume of pornographic spam, defined as adult or sexually explicit content intended for people over the age of 18, represented the largest percentage (17.7%) of unsolicited email. Coming in close behind was spam for cosmetics and/or Viagra ads (12.59%), medical (11.64%), and general shopping ads (11.28%). As shown in the pie chart below, Websense Security Labs classifies spam into the following 16 categories:

Q4 Spam Classifications



Websense Security Labs expects hackers to increasingly use Web spam to drive traffic to infected sites for malicious purposes. As of today, 65% of unwanted messages contain links to Web sites, including links to spam and malicious sites. As the percentage of spam messages with images increases (32%), organizations will need to adopt measures to eliminate spam and malware before it hits to the network or risk increased email bandwidth and storage costs.

Q4 Spam Types



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.

Unique Attack Methods

This section of the report is focused on tracking unique, unusual or new attack methods discovered during the second half of 2007. Given the volume of attacks, we have chosen to highlight what we consider to be two of the most unique attacks.

Ransom Encryption

Some attackers became more aggressive this summer by choosing to use scare tactics over technical sophistication in hopes of turning a quick profit. Using a Trojan horse, attackers scanned user hard drives for files to encrypt from a .tmp file. They led their victims to believe that their private data had been compromised and encrypted with a 4096bit RSA key, a high level of encryption. In the blackmail message below, hackers claimed that they would publicly share their victim's private data on the Internet if they didn't purchase their decryption software to restore their files.

```
Hello, your files are encrypted with RSA-4096 algorithm
(http://en.wikipedia.org/wiki/RSA) .

You will need at least few years to decrypt these files without our
software. All your private information for last 3 months were
collected and sent to us.

To decrypt your files you need to buy our software. The price is $300.

To buy our software please contact us at: tristanniglam@gmail.com and provide us
your personal code [REDACTED]. After successful purchase we will send
your decrypting tool, and your private information will be deleted
from our system.

If you will not contact us until 07/15/2007 your private information
will be shared and you will lost all your data.

Glamorous team
```

In June, Websense Security Labs was the first to discover that hackers were not actually using the sophisticated encryption algorithm that they touted in their message. Websense Web security customers were protected against this attack. For more information on the attack analysis conducted by Websense visit: <http://www.Websense.com/securitylabs/blog/blog.php?BlogID=136>

Sending Out an SOS (Spam Over Skype)

Websense Security Lab researchers discovered an attack that illustrates a new avenue for spam by propagating through Skype, a software that enables users to make free telephone calls to other Skype users over the Internet. ThreatSeeker technology found that malware authors utilized social-engineering methods to pass their malware off as legitimate software to unsuspecting victims. Users were lured to click a malicious link from "Scan Alert" warning of a malware infection. Upon clicking the link, the Web site generated misleading results from a fake virus/malware scan. If users attempted to remove the results they were prompted for credit card information and were tricked into paying to infect their own computer.

Skype's directory listing allows anyone to search for any name/keyword and directly contact that person with a link embedded in the message. Websense Web security and messaging security customers were blocked from ever reaching these malicious sites. For more information on the analysis conducted by Websense on this attack visit: <http://www.Websense.com/securitylabs/blog/blog.php?BlogID=151>



Websense Security Labs Firsts

Websense Security Labs pioneered the first phase of Web attack identification with its Web classification and security intelligence. Using an array of machines and techniques, ThreatSeeker™ technology preemptively mines the Web, searching for malicious sites, content, and known and emerging threats. The following list highlights the major attacks successfully identified by Websense Security Labs before any other research team during the second half of 2007.

United Nations – Asia Pacific HIV/AIDS Portal Compromise

Attack Date: August 27, 2007

Websense Security Labs discovered that the United Nations' HIV/AIDS portal for Asia Pacific was compromised with a malicious script that attempts to exploit multiple vulnerabilities.

Attack Details: Websense ThreatSeeker technology discovered that when users visited the UN Web site, a malicious JavaScript file (e.js) was executed creating two additional iframes in the page. Unprotected site visitors inadvertently downloaded a Trojan that infected their desktops with malicious code. Victims became unwilling participants in a larger bot network that could have been potentially used for future malicious attacks. Websense researchers believe that these hackers are the same perpetrators behind two similar compromises, one of a prominent bank in India and the other of a large industry organization Web site that the Websense Security Labs discovered and reported upon during the first half of 2007. Luckily, Websense Web Security customers were protected against all of these attacks.

Phast Phlux Phishing

Attack Date: Sep 13 2007

After MySpace announced increased measures to protect the MySpace community from online threats, many users of the popular social-networking site were compromised by a scam that stole confidential user logon credentials for malicious purposes. Ironically, MySpace users were attacked by deceiving URLs that mimicked the outbound msplinks.com links that MySpace implemented to curb spam and phishing attacks. (The msplinks.com service is provided by MarkMonitor to safely redirect MySpace users to sites outside of MySpace.)

Attack Details: Websense ThreatSeeker technology found that the attackers used multiple DNS A records with low TTL's (Time to Live) (a fast moving attack that is difficult to catch) to target victims. Researchers found the malicious Web site's source code was almost identical to the source code of the real myspace.com page, with virtually all the <a href> tags linking back to myspace.com—except for the email and password form. The domains hosting these phishes resolved to numerous IP addresses that were constantly changing, an indicator of a fast-flux service network. Although the malicious domain was Chinese, the hosts were most likely desktops in various countries with broadband Internet, belonging to casual Web surfers at home who became unwilling participants in this orchestrated phishing attack. The victims had their MySpace profiles infected—including the users on their "friends list"—which spread the attack virally and increased the infections exponentially. , Websense Web Security customers were conveniently protected from this Web 2.0 attack.

Halloween Deception: Information-Stealing Trojan

Attack Date: October 29, 2007

Hackers, masquerading as the Internet directory service Yahoo, went trick-or-treating before Halloween for personal banking information. Users without adequate protection were tricked into downloading a Trojan horse onto their machine that was designed to steal sensitive banking information, including passwords, credit cards, and online banking information.

Attack Details: Websense Security Labs discovered the email lure by using the combined research intelligence from Websense Hosted Web Security, Websense Hosted Email Security, and ThreatSeeker technology. The Trojan horse was emailed out as a Yahoo Halloween greeting card in Mexico. This attack targeted unsuspecting Mexican users of Yahoo that trusted the company's brand reputation

Websense identified four main sites hosting the same malicious binary in Korea, Brazil, and Russia. The file that had an MD5 of 65cd5a35bc70075f86cb6404f54d67b8 was named "halloweenDay.exe" and was poorly detected by antivirus signatures. Users without adequate email and Web security protection that visited the site and ran the file were impacted by this attack. Fortunately, Websense Web and Messaging Security customers were protected against this attack.

Websense has a unique, early insight into email and Web threats that provides comprehensive protection for all customers across both protocols.

Department of Justice Trojan Horse

Attack Date: December 3, 2007

Websense Security Labs discovered a new email attack variant similar to attacks previously launched on the IRS and Better Business Bureau. At the time of discovery, none of the major antivirus vendors had detected the malicious code. The spoofed email claimed to be from the United States Department of Justice (USDOJ). Websense Security Labs have been tracking these attacks and have previously reported on them on our site.

Attack Details: Websense Security Labs discovered the email lure by using the combined research intelligence from Websense Hosted Web Security, Websense Hosted Email Security and ThreatSeeker technology. The message claims that a complaint to the USDOJ has been filed against the recipient's company. The email informs the reader that a copy of the original complaint has been attached to the email. The attached "complaint" is a Trojan .scr file with an MD5 of 083cdbc8b8cac465dc130348f88ac48d. The .scr file created a second file named xp2007.dat in c:\ which was then silently added as a Brower Helper Object in Internet Explorer. Again, Websense Web Security and Messaging Security customers were protected against this attack.

A Look Forward

Organizations around the world rely on Websense to best protect employees, critical applications and confidential data from increasingly sophisticated and dangerous Internet threats. The predictions contained within this report are based on analysis of current attack trends, cybercriminal techniques and threat intelligence gathered by researchers with Websense Hosted Web Security and Websense Hosted Email Security.

WebSense Security Labs Anticipates the Following in 2008:

1. Olympics – new cyber attacks, phishing and fraud

Event-based attacks and scams are popular, and with the whole world watching, the 2008 Olympics may fuel a surge in cyber attacks. As the Olympic torch burns, Websense researchers predict the possibility of large scale denial of service attacks on Beijing Olympic-related sites as political statements and fraud attempts through email and the Web surrounding the Olympics. Additionally, Websense predicts compromises of popular Olympic news or other sports sites—attacks designed to install malicious code on end-users machines and steal personal, business, and confidential information.

2. Cross platform Web attacks – Mac, iPhone popularity spurs increase

With the brand-popularity and growing use of iPhones and Macintosh computers, Websense researchers predict attackers will increasingly launch cross-platform Web attacks that detect the operating system in use and serve up code specifically targeting that operating system instead of attacks based on just the Web browser. Operating systems that are targeted now include Mac OSX, iPhone, and Windows.

3. Malicious spam invades blogs, search engines, forums and Web sites

Websense predicts that hackers will increasingly use Web spam to post URLs to malicious sites within forums, blogs, in the commentary or "talk-back" sections of news sites and on compromised Web sites. This activity not only drives traffic to the infected Web sites but also assists in pushing the purveyor's site rating higher on search engine rankings, increasing the risk that users will visit the site.

4. Attackers use Web's 'weakest links' to launch attacks

The Web is an entanglement of links and content. The advent of Web 2.0 additions such as Google AdSense, mash-ups, widgets, and social networks along with the massive amounts of Web advertisements linked to Web pages have increased the likelihood of 'weak links'—or Web sites and content that are vulnerable to compromises. Websense predicts that attackers will increasingly exploit the weakest links within the Web infrastructure in order to target the greatest number of Internet users. Most vulnerable to these attacks are search engines and large-user networks such as MySpace, Facebook or other social networking sites.

5. Number of compromised Web sites will surpass number of created malicious sites

The Web as an attack vector has been steadily increasing for the last five years and now attackers are using

compromised sites as their launching platforms—even more than their own created sites. Compromised sites—particularly, sites well-visited by end-users, such as the Dolphin Stadium attack that occurred a few days prior to the 2007 Super Bowl XLI in Miami, provides attackers with built-in Web traffic and minimizes the need for lures through email, instant messaging or Web posts.

Websense Security Labs researchers gather threat intelligence with Websense ThreatSeeker technology, which scans more than 600 million Web sites per week searching for malicious code, along with Websense's Hosted Email Security, which scans more than 350 million emails per week for email security threats.

6. Rise in targeted Web 2.0 special-interest attacks—hackers targeting specific groups of people based on interests and profile

Web 2.0 has spawned a proliferation of Web users that visit chat rooms, social networking sites, and special interest Web sites such as travel sites, automotive, and more. These sites provide hackers with potential victims that fall within a certain age group, wealth bracket, or people with particular purchasing habits. In 2008, Websense researchers predict targeted attacks will rise toward specific social networking or special interest sites that have a higher probability of delivering a payoff.

7. Morphing JavaScript to evade antivirus scanners

Hackers are upping the ante with evasion techniques that use poly-morphic JavaScript (Polyscript), which means that a uniquely-coded Web page is served up for each visit by a user to a malicious Web site. By changing the code every visit, signature-based security scanning technologies have difficulty detecting Web pages as malicious and hackers can extend the length of time their malicious site evades detection.

8. Data concealment methods increase in sophistication

Websense predicts an increased use of crypto-virology and sophistication in data concealment including the use of steganography, embedding data within standard protocols, and potentially within media files. Toolkits widely available on the Web will be used to embed proprietary information and steal data.

9. Global law enforcement will crack down on key hacker groups and individuals

In 2007, large-scale Internet-based attacks garnered the attention of law enforcement officials around the world. Websense anticipates that through the global cooperation of enforcement agencies the biggest crackdown and arrests of key members of a hacker group will occur in 2008.

10. Vishing and voice spam will combine and increase

The vast cell phone user population has grown into a lucrative market to exploit with spamming and “vishing” for financial gain. To date, researchers have seen an increased number of vishing attacks but not a lot spam—or proactive automated calling. In 2008 Websense predicts that “vishing” or the practice of using social engineering and Voice-over-IP (VoIP) to gain personal and financial information, as well as voice spam, will combine and increase—users will receive automated voice calls on LAN lines with voice spam to lure them to input their credentials through the telephone.

Websense Security Labs will continue to issue security alerts to the security community and Websense customers about malicious Web sites, phishing-based attacks, and other emerging Internet threats.

Summary

During the second half of 2007 the Web continued to be the largest attack vector with more and more good sites going bad. Websense Security Labs found that 51% of the sites they classify as malicious have been compromised. Hackers exploited the use of professional toolkits and organizations were plagued with the widespread nature of the Storm attacks. Websense Security Labs believes organizations should brace for similar, continuing challenges in 2008. Hackers will continue to get creative and leverage user-created content and Web 2.0 applications to create even bigger security concerns for organizations. 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.

About Websense Security Labs

Websense Security Labs is the security research arm of Websense, Inc. (NASDAQ: WBSN) 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.

Recently the Websense Security Labs team has expanded to include an advanced content and email research team. By combining Web and email research, Websense has a unique, early insight into email and Web threats that provides comprehensive protection for all customers across both protocols.

Websense Security Labs – a Pioneer in Emerging Threat Protection

- 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

Websense Security Labs researchers gather threat intelligence with Websense ThreatSeeker technology, which scans more than 600 million Web sites per week searching for malicious code, along with Websense’s Hosted Email Security, which scans more than 350 million emails per week for email security threats. The Websense Security Labs research team, credited with finding several high-impact Web exploits and zero-days, sends out an average of 80 security updates per day, to protect more than 42 million employees from external and internal computer security threats.

Security Alerts & More

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>