



A Websense® White Paper

Websense Security Labs

State of Internet Security, Q1 – Q2, 2009

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, email and data content—providing Websense with unparalleled visibility into the state of content on the Internet and in email.

This report summarizes the significant findings of Websense researchers using the ThreatSeeker Network during the six-month period ending June 2009.

Websense ThreatSeeker Network Research Highlights, Q1 - Q2 2009

Web Security

- Websense Security Labs identified a 233 percent growth in the number of malicious Web sites in the last six months and a 671 percent growth during the last year.
- 77 percent of Web sites with malicious code are legitimate sites that have been compromised. This remains unchanged from the last six-month period.
- 61 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.
- 95 percent of user-generated comments to blogs, chat rooms and message boards are spam or malicious.
- 50 percent of Web pages linked to Web sites categorized as “Sex” also served malicious content.
- 69 percent of all Web pages with any objectionable content (e.g. Sex, Adult Content, Gambling, Drugs) also had at least one malicious link.
- 78 percent of new Web pages discovered in the first half of 2009 with any objectionable content had at least one malicious link.

Email Security

- 87.7 percent of email messages were spam. This represents a three percent increase over the last six months.
- 85.6 percent of all unwanted emails in circulation during this period contained links to spam sites and/or malicious Web sites.
- Shopping remained the leading topic of spam (28 percent), followed closely by cosmetics (18.4 percent), medical (11.9 percent) and education (9.5 percent). Education themed spam has nearly doubled over the previous period and may be related to the recession as spammers seek to exploit people looking to gain new skills or obtain fake qualifications to help their job prospects.

Data Security

- 37 percent of malicious Web/HTTP attacks included data-stealing code. This remains unchanged from the last six-month period.
- 57 percent of data-stealing attacks are conducted over the Web. This number has stayed consistent over the six-month period.

A Look Back at the Last Six Months

Blended Threats

Blended threats continued to dominate the security landscape in the first half of 2009 with 85.6 percent of all unwanted emails in circulation during this period containing links to spam sites and/or malicious Web sites. These threats have continued in the past year and further illustrate that Web security intelligence is a critical component of email and data security.

Web 2.0 Security Trends

Web 2.0 sites (sites that allow user-generated content) comprise many of the most visited sites on the Internet. The very aspects of Web 2.0 sites that have made them so revolutionary – the dynamic nature of content on the sites, the ability for anyone to easily create and post content, and the trust that users have for others in their online networks – are the same characteristics that radically raise the potential for abuse. Web 2.0 sites are increasingly being used to carry out a wide range of attacks. For example, in January, hackers targeted Twitter users in a bid to steal account information. The hackers exploited the trust that Twitter users place in their network of friends and followers by using the direct message function to send phishing lures to followers.

Efforts to self-police these Web 2.0 properties have also been largely ineffective. Websense research during the period showed that community-driven security tools (asking users to report inappropriate content) on sites like YouTube and BlogSpot are 65 percent to 75 percent ineffective in protecting Web users from objectionable content and security risks.

Even the trusted social networking site Facebook was not immune to Web-based threats, with the Koobface attack and other rogue applications created to steal Facebook users' login credentials.

Websense Security Labs research also discovered that more than more than 200,000 phony copycat sites have been created, all including the terms Facebook, MySpace or Twitter in their URLs. These sites are created by fraudsters seeking to take advantage of the huge number of users of social networking sites. Facebook copycat sites lead the sector with more than 150,000 known fake URLs charted during the research period. Examples include URLs like buy.viagra.twitter.fakedomain1234.com or hotbabesofmyspace999.com. These “blackhat search engine optimization” techniques are designed to drive traffic to dubious sites.

Attackers Capitalize on News Events and Celebrities

Attackers also capitalized on major events during the last six months, such as the economic recession, to take advantage of job seekers looking for employment by using various exploits to infect victims' computers.

Celebrities and politics continued to be used as lures by spammers and cybercriminals. At the end of June, the sudden death of Michael Jackson prompted spammers to send malicious email messages using news of the event as a social engineering technique to lure people to their sites. Earlier in the year, malicious hackers leveraged the arrival of Barack Obama into office by registering multiple bogus user accounts on My.BarackObama.com in an effort to spread malicious code around the Web.

Attack Tactics

Visual social engineering tactics - which include tricking users into downloading fake video player codecs or Flash or Adobe Acrobat updates, but instead deliver malware - were used by spammers and malware authors to target popular sites including Digg, LinkedIn and Classmates.

On the data security front, SQL injection attacks over the Web were used to infect and steal sensitive credit card information in unprecedented quantities. These massive data breaches, such as the theft at Heartland Payment Systems – potentially the largest data breach ever -- illustrate the dangers of data attacks over the Web and the need for ongoing monitoring of data traveling out of an organization through Web traffic.

Mass Web Attacks

In the first half of the year, Websense Security Labs saw the use of widespread attacks aimed at compromising the largest number of Web sites possible. The major attacks, including: Gumblar, Beladen and Nine Ball compromised hundreds of thousands of trusted and known Web properties with massive injection campaigns that infected users who simply visited these sites.

Perhaps most telling on the Web security front is the fact that Websense Security Labs identified a 233 percent growth in the number of malicious sites in the last six months and a 671 percent growth over the last year.

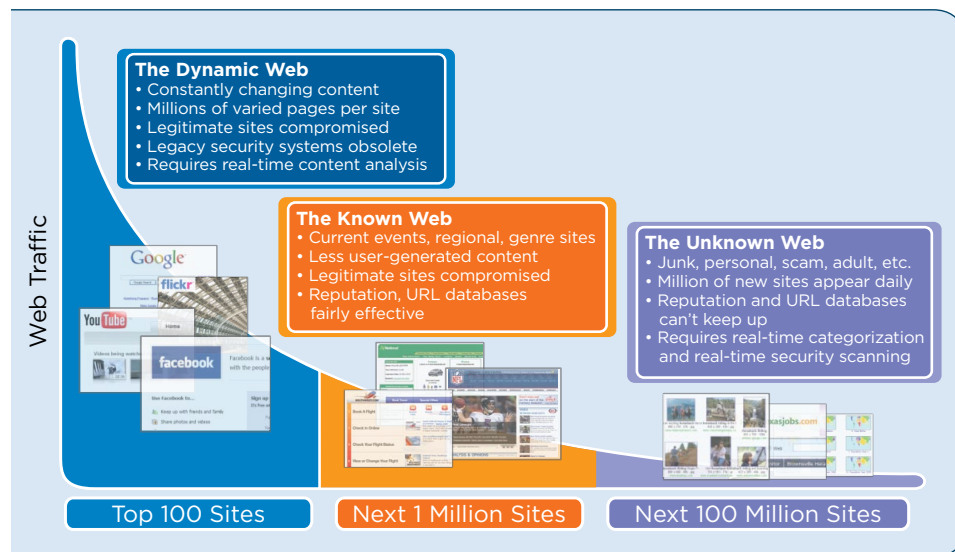
Web Security

Changes in the Threat Webscape

Websense Security Labs classifies the Webscape into three general sections:

- The top 100 most visited Web properties, which tend to be classified as “Social Networking” or “Search” sites.
- The next million most visited sites are primarily current event and news sites and are more regional and genre-focused.
- The “long tail” of the Internet is populated by personal sites like blogs, small business sites and Web sites established specifically for fraud and abuse.

Each area of the Webscape has its own unique security challenges but 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 authors of malicious code with abundant opportunity to easily reach a wide number of victims with their attacks. Research shows that attackers focus their attention on these interactive Web 2.0 elements of the evolving Webscape, demonstrating that businesses need to be able to scan and classify the content of Web sites in real time in order to protect their networks and their essential information from Web threats.



- **More than 47 percent of the top 100 sites support user-generated content.**
- **Not surprisingly, sites that allow user-generated content comprise the majority of the top 50 most active distributors of malicious content.** Blog hosting sites that offer free hosting and good reputations provide malware authors with the perfect combination to compromise unsuspecting users.
- **61 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.** In many cases these redirects appeared as the actual Web site, when in fact the content served on that page was being hosted elsewhere.
- **Websense Defensio technology** enabled Websense Security Labs to identify a significant and alarming trend regarding the ease with which Web 2.0 sites can be compromised: **95 percent of user generated comments to blogs, chat rooms and message boards are spam or contain malicious links.**

Many of the top compromised categories of Web sites are found within the “long tail” of the Internet:

- **Sex, advertisements, business and economy, IT, and travel** made up the most commonly compromised categories of Web content.
- **50 percent of Web pages with a link categorized as “Sex” also have at least one malicious link.** The term “malicious” typically refers to links that have specific, hidden exploits that target a user’s computer.

But it is not just Web sites categorized as “Sex” that are a haven for malicious links:

- **69 percent** of all Web pages with any objectionable content link (e.g. Sex, Adult Content, Gambling, Drugs) also served malicious content.

And the problem seems to be growing:

- **78 percent of new Web pages discovered in the first half of 2009 with objectionable content** (such as pornography, sex or gambling sites) also have at least one malicious link.

The Websense Security Labs is seeing that the increasing popularity of social networking and Web 2.0 sites has helped fuel another trend that could also be described, as “hateful” in spirit:

Researchers at Websense Security Labs have seen a substantial increase in the occurrence of hate or militant content residing on Facebook and other popular Web 2.0 sites such as YouTube, Yahoo! Groups and Google Groups. In fact, looking at the Websense categories “Militancy and Extremist” and “Racism and Hate” from January through May 2009:

- Websense saw a 326 percent increase in cyber terrorism (militancy and extremists Web sites) over the same period in 2008.
- Websense is now tracking approximately 15,000 of these hate and militancy sites, with 1,000 added in just the first six months of this year.

Web 2.0 and Business – Increased Opportunity and Increased Risk

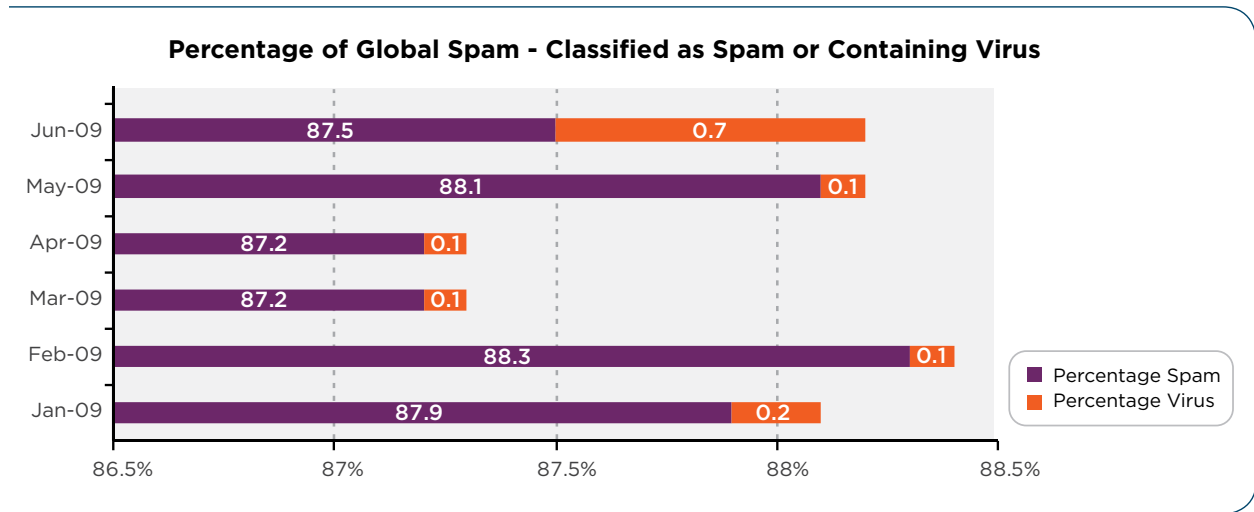
Like it or not, Web 2.0 is quickly becoming “Enterprise 2.0” as a growing number of Web applications make their way into the corporate environment. Many business experts recommended that organizations should embrace the value of Web 2.0 tools as a way to help lower costs and increase collaboration with little to no administrative burden on IT staff.

Websense conducted its own “Web 2.0 @ Work” survey, discovering that 95 percent of organizations allow access to some types of Web 2.0 sites or applications, and 62 percent of IT managers believe that Web 2.0 is necessary to their business. Sixty-four percent of IT managers responded that they permit access to social networking sites primarily used for business, such as LinkedIn. Despite widespread adoption of Web 2.0, a startling 91 percent of businesses surveyed in the Web 2.0 @ Work study

responded that they do not have the necessary security to protect from all Web 2.0 threat vectors across Web, email and data security.

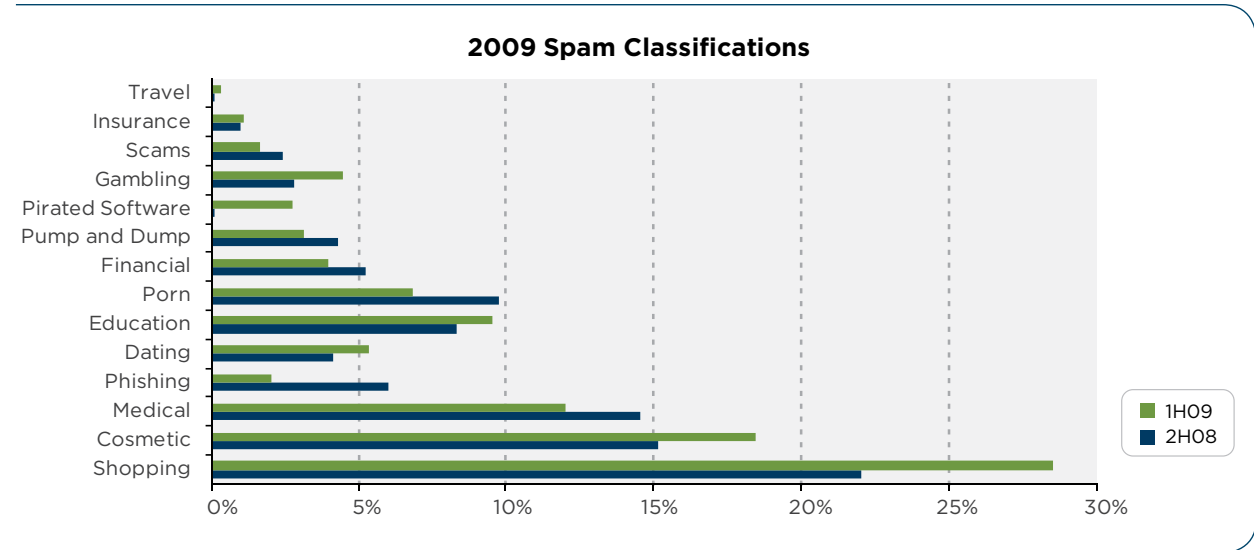
Email Security

As stated previously, spam continues to comprise the majority of emails with some 87.7 percent of email messages classified as spam over the last six months. This represents a three percent increase over the previous period, despite ongoing attempts to shut down major spam servers. Blended threats — emails that contained links to spam sites and/or malicious Web sites — comprised 85.6 percent of all unwanted emails in circulation during this period.



The three most popular topics for spam remained shopping (28 percent), cosmetics (18.4 percent) and medical (11.9 percent.) Over the last six months, the growing category of education spam accounted for 9.5 percent of all spam and could be attributed to the recession. Spammers have been targeting the unemployed who are looking to re-train or gain qualifications to help their job prospects.

As shown in the bar chart below, WebSense Security Labs classifies spam into the following 14 categories:

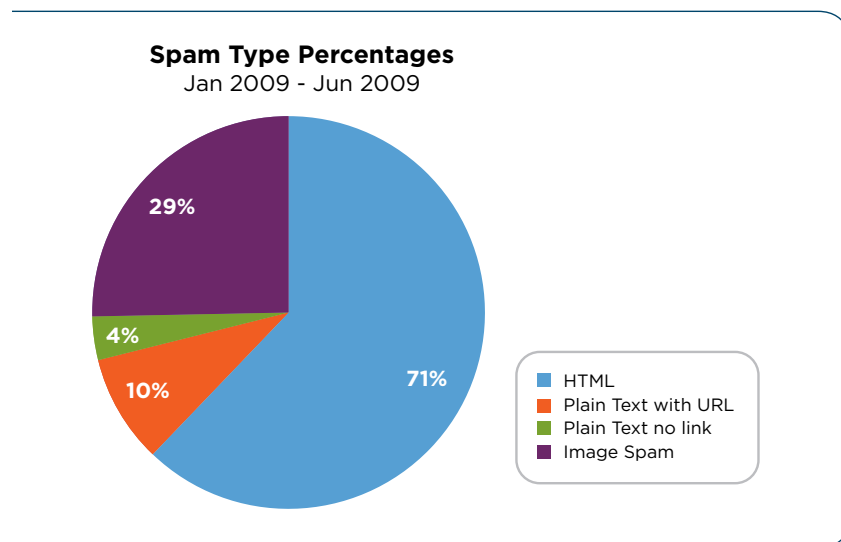


Spam Types

For quite some time, Websense Security Labs has seen spammers and malware authors adapt their techniques by moving to non-email spamming tactics, including attacks on Web 2.0 sites, as illustrated by Twitter, Facebook, and Orkut-based attacks.

In the first half of this year fraudsters also used more image spam and ramped up their HTML spam, often in attempts to evade spam blocking measures.

- HTML spam increased 7.9 percent, while plain text with URL dropped 57.2 percent.
- Image spam increased 70.6 percent, while plain text with no URL dropped 59 percent.



Websense Security Labs saw an increase in the number of phishing emails using attached HTML forms and many companies were hit by spear phishing campaigns. Also, the spam trends in the first half of 2009 culminated in a huge spam influx in the month of June. The total number of emails detected as containing viruses increased six-fold in this month. Major news events, such as an Air France plane crash and the death of Michael Jackson also led to a multitude of targeted spam campaigns. Following his death, researchers saw the continued use of Michael Jackson's name as a lure to promote everything from pharmacy Web sites to malicious downloads hosted on sites created specifically for that purpose.

Spam Innovation

Spammers' efforts to reach their prospective customers continued with increased creativity and complexity. The long battle between service providers and spammers was evident when spammers once again successfully broke Microsoft's revolutionized CAPTCHA, most recently in February of this year.

Spammers are also adapting by attempting to increase the overall time a spam campaign survives and by making the campaign increasingly difficult to trace back to its origins, as demonstrated by Waledac's Valentine's Day campaign.

Visual social engineering tactics, which may involve getting users to download fake video player codecs or Flash or Adobe acrobat updates but instead deliver malware, are also being used by spammers to increase the success of their attacks. This tactic was evident in a Skype Valentine spam lure, a Wal-Mart fake survey and spam campaigns with malicious zip attachments that appeared to be sent from legitimate users.

Phishing

While phishing attacks decreased to a third of their level six months ago, to 2 percent of all emails, in their place Websense Security Labs detected an increased use of data-stealing Trojans and DNS poisoning tactics to lure victims to malicious sites, indicating a move to gain sensitive user information.

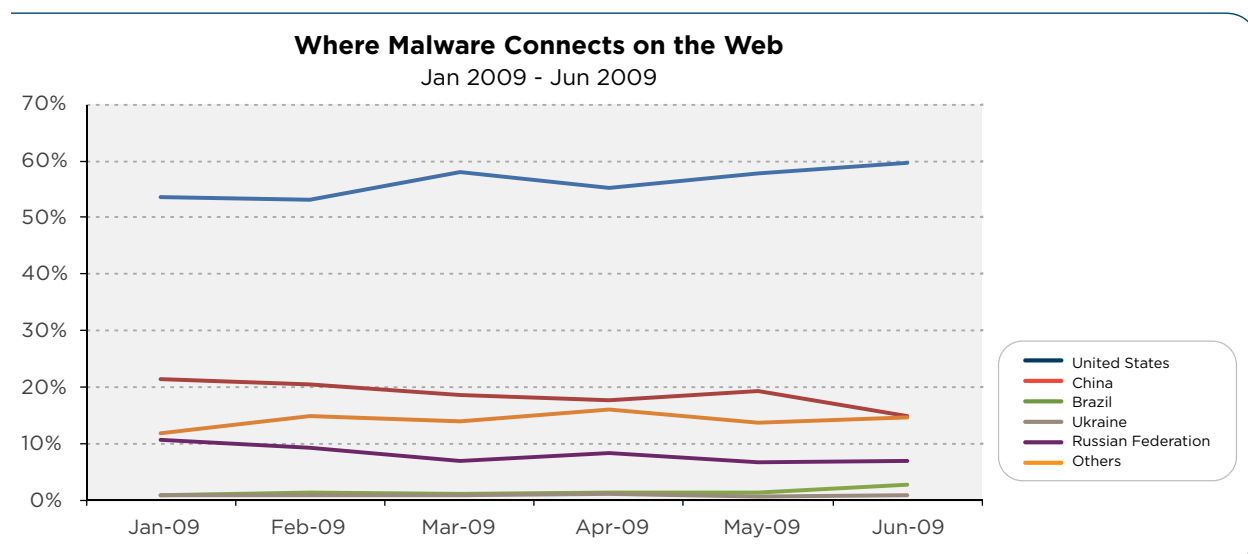
Despite the decrease in number of phishing attacks, phishers worked to improve their odds of success by using timely and believable topics such as a tax season phishing campaign luring victims to download and submit a fake economic stimulus payment form.

Phishers also targeted GTalk and Gmail accounts where the victim received a GTalk IM with a TinyURL link that redirects to a ViddyHo login page. The attack aimed to steal Google usernames and passwords, however unlike previous phishing attacks, this one has strong monetary ties as Google credentials can be used in Google Checkout and Google AdSense accounts.

Researchers from Harvard and Cambridge estimate that 75.8 percent of phishing sites are hosted on compromised servers. It is possible that phishers have obtained access to such servers by using Google hacking techniques – an attempt to use Google Search and other Google applications to find security holes in the configuration and computer code that Web sites use. The effectiveness of such techniques is notable given the fact that most SQL injection attacks in 2008 performed automatic search engine reconnaissance.

Data Security

The exposure of confidential information is now the single greatest threat to enterprise security. According to research conducted by Websense Security Labs, **57 percent of data-stealing attacks are conducted over the Web.** With data-stealing Web and email attacks on the rise, Websense Security Labs is tracking where data is being sent around the globe.

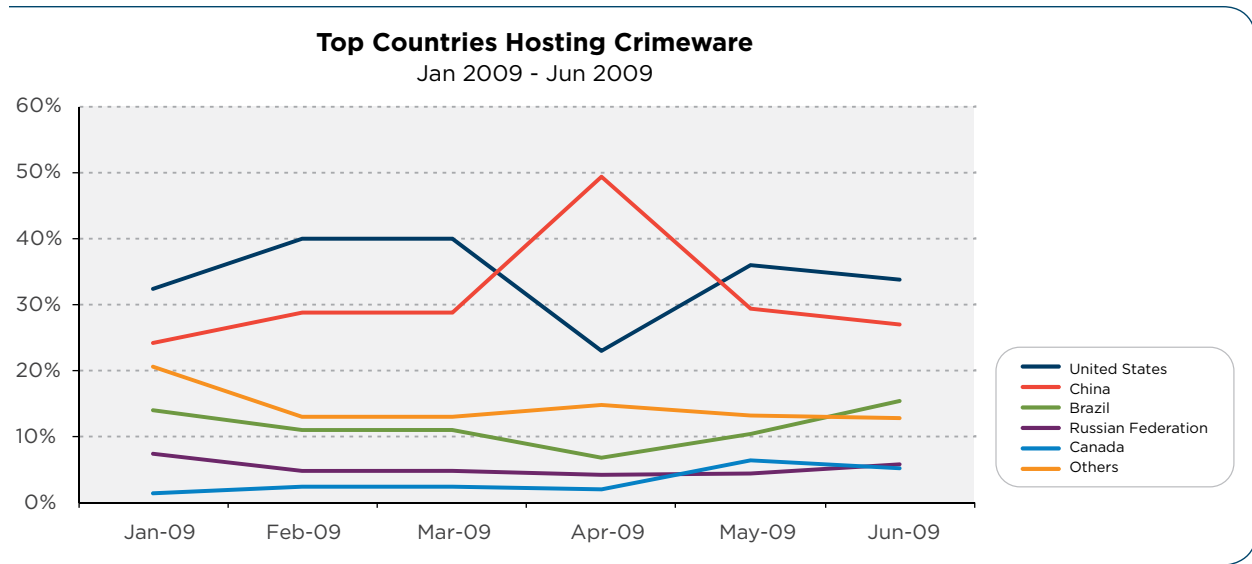


In the past six months and moving forward, Websense Security Labs expects to see less malware connecting to the United States as other countries' infrastructures improve and attackers start spreading their hosting locations around the world. As noted in the last report, the spike in malware from the United Kingdom dropped from the previous six month period back down to 1.3 percent for a 14.7 percent decrease. China had a seven percent increase from the previous six month period.

Flawed Security Sites: Top Countries Hosting Crimeware

Crimeware is a class of malware designed specifically to automate cybercrime. Distinct from spyware, adware and malware, crimeware is designed to perpetrate identity theft in order to access a computer user’s online accounts and enrich the thief controlling the crimeware.

In addition to tracking where stolen data is sent, Websense Security Labs also tracks where other forms of crimeware are hosted, and the United States leads the pack:

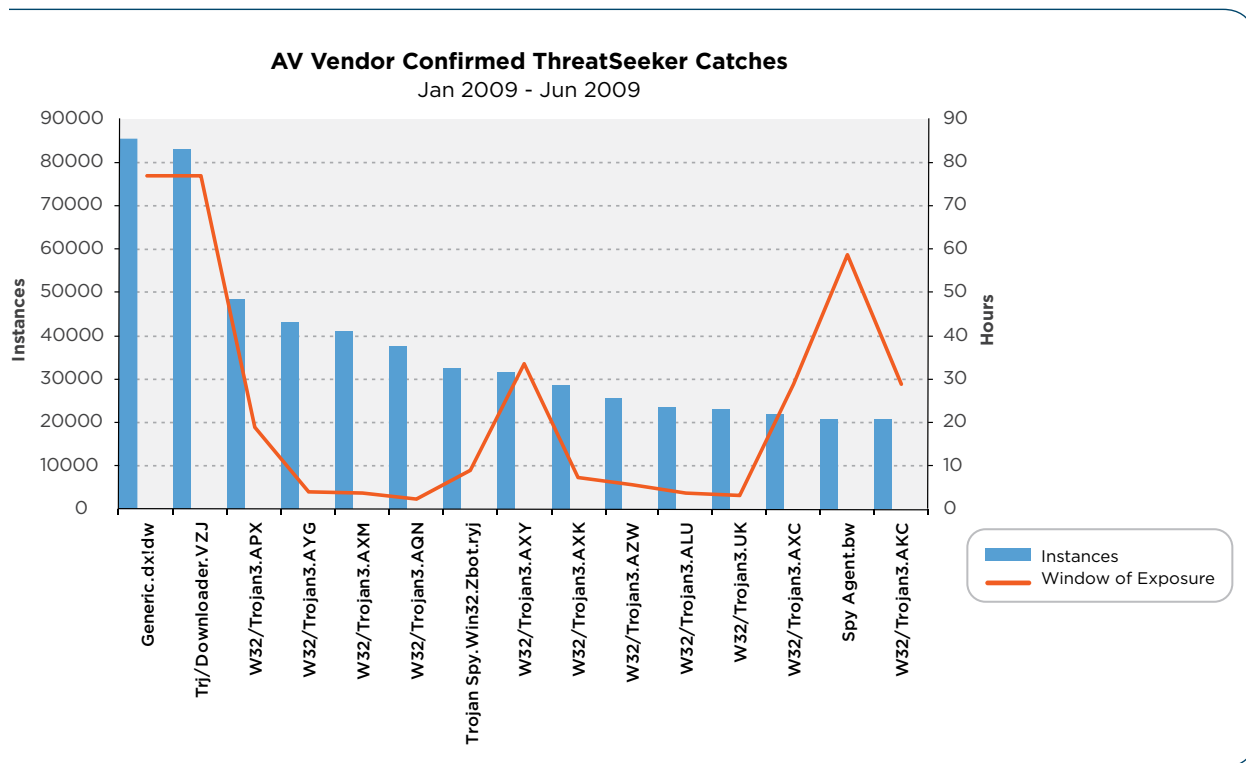


An example of this crimeware in action is the recent case involving a major online bill-pay provider, CheckFree. Hackers seized control of the CheckFree Web site and redirected visitors to a malicious Web site hosted in Ukraine that tried to install malware on the visitors’ computers. This was a huge attack, as CheckFree reportedly has more than 24 million customers and controls 70 to 80 percent of the U.S. online bill-pay market.

Websense Security Labs Firsts

From ThreatSeeker Discovery to Signature: Window of Vulnerability

The Websense ThreatSeeker Network discovers many malicious applications being circulated via email, drive-by downloads, exploit code and other mechanisms employed by creative malware authors. In the last six months the ThreatSeeker Network **detected 922,433 instances of 623 unique pieces malware** before antivirus vendors. Websense security supplements outdated antivirus software by seeking out threats before customers are infected and providing protection within minutes of discovery. The chart below shows the window of exposure between threat detection by Websense ThreatSeeker Network and the release of the signatures by antivirus software providers. **The average window of exposure for antivirus signatures to be created during the first half of 2009 was 22 hours.**



The following list highlights a few of the major attacks discovered by WebSense Security Labs during the first half of 2009.

Barack Obama’s Site Leading to Trojan Horse

Attack Date: 01/26/2009

Attack Details: WebSense Security Labs ThreatSeeker Network detected that malicious hackers registered multiple bogus user accounts on My.BarackObama.com (an online community for citizens to rally behind President Obama) in order to spread malicious code around the Web. Hackers created blogs on My.BarackObama.com with a fake YouTube image, enticing visitors to “Click here to see movie.” Clicking on the link lead visitors to a Web site using YouTube’s template for viewing online videos, except on this site the videos were filled with pornography. Clicking on the video to view results prompted the browser to download a video codec, which was really a malicious Trojan executable file. The malicious campaign didn’t end there. My.BarackObama.com is a highly visible, reputable and popular Web site with almost 9,000 other sites linking to it. The hackers sprayed the malicious URLs all over the Web by injecting them onto blog comment forms and other content management systems commonly used by Web 2.0 sites. The malicious code had less than a 35 percent detection rate by the major antivirus vendors. This campaign is an example of how attackers are using Web 2.0 functionality to reach victims in new ways. For more details on this compromise, view the alert [here](#).

eWeek Web Site Leads Users to Rogue Anti-Virus (AV) Application

Attack Date: 2/24/09

Attack Details: WebSense Security Labs ThreatSeeker Network discovered that the eWeek.com Web site served malicious advertisements (malvertisements) to visitors through Google/DoubleClick’s ad network. Google acknowledged the existence of the malvertising scourge on its ad network. WebSense alerted officials at eWeek who worked with Google to rectify the situation immediately.

Mass Fake Delta Airlines Ticket Confirmation Email Message

Attack Date: 03/05/09

Attack Details: Websense Security Labs ThreatSeeker Network discovered a scam involving the spread of email messages disguised to look as if they were from Delta Airlines. Within one week, the Websense Security Labs team received more than 3000 samples. The email messages had the subject “Confirmation of ticket purchase at www.delta.com” and asked recipients to print a supposed “Passenger Itinerary Receipt” attached to the message. The attachment was actually a Trojan file. For more information about this attack, view the alert [here](#).

Koobface - On the Run Again

Attack Date: 05/26/09

Attack Details: Since 2008, Websense Security Labs ThreatSeeker Network has monitored the spread of Koobface via Facebook, Friendster, MySpace, hi5, Bebo and other social networking sites. In May, Koobface attempted to run another campaign on Facebook. If infected, Facebook users started to spam their friends with a link to a malicious Web site. When users visited the link, they were redirected to various malicious and phishing pages. Websense Security Labs detected these pages on numerous .be domains and TinyURL links. One such malicious page is a fake YouTube page that appears to be a funny video. The page tells visitors to upgrade their Flash player in order to play the video, but the fake Flash setup program is actually Koobface malware. Users who execute the setup.exe file infect their computer and download fake antivirus software. For more details on this compromise, view the alert [here](#).

Beladen Mass Compromise

Attack Date: 06/01/09

Attack Details: Thousands of legitimate Web sites were discovered to be injected with malicious JavaScript code that lead to an active exploit site. At least 40,000 hacked sites shared similar code masquerading as legitimate Google Analytics HTML code.

In a matter of microseconds, the malicious site redirected users to a fake Google Analytics page that would chart the activity, and then forward them to the Beladen payload site. Once at the site, the script would check for a list of 15 to 20 known unpatched vulnerabilities to infect the visitor. If these attempts failed, the site would flag the user with a bogus virus alert and a pitch to install a rogue antivirus program. For more details on this compromise, view the alert [here](#).

Nine-Ball Mass Compromise

Attack Date: 06/16/2009

Attack Details: In June, the Websense Security Labs ThreatSeeker Network detected a large mass injection attack designed to steal user information “in the wild.” More than 40,000 legitimate Web sites were compromised ending in a series of drive-by exploits that, if successful, installed a Trojan downloader on the user’s machine. For more details on this compromise view the alert [here](#).

Michael Jackson Death Prompts Malicious Spam

Attack Date: 06/26/2009

Attack Details: After the death of Michael Jackson was confirmed, Websense Security Labs discovered malicious spam emails offering recipients links to unpublished videos and pictures of the singer. The spam email appeared to offer a link to a YouTube video, but instead sent the recipient to a Trojan downloader hosted on a compromised Web site. For more details on this compromise view the alert [here](#).

About Websense

Websense, Inc. (NASDAQ: WBSN), a global leader in integrated Web, data and email security solutions, provides Essential Information Protection™ for approximately 44 million product seats under subscription. 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 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.

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>.