A Websense® White Paper

Websense Security Labs

State of Internet Security, Q3 – Q4, 2009

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, 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 December 2009.

Websense ThreatSeeker Network Research Highlights, Q3 – Q4 2009

Web Security

- 13.7% of searches for trending news/buzz words (as defined by Yahoo Buzz & Google Trends) led to malware.
- While the first half of 2009 saw a sharp rise in the number of malicious Web sites, the second half of the year revealed a 3.3% decline in growth. Websense Security Labs believes this is due to the increased focus on Web 2.0 properties with higher traffic and multiple pages. Websense Security Labs has identified:
  - Gumblar, Beladen, Nine Ball and other mass injection campaigns led to a higher number of attacks in April & June over other months.
  - Overall, comparing the second half of 2009 with the same period in 2008, we have seen an average of 225% growth in malicious Web sites.
- 71% of Web sites with malicious code are legitimate sites that have been compromised.
- 95% of user-generated posts on Web sites are spam or malicious.
- Consistent with previous years, the majority of malware still connects to host Web sites registered in the US (51.4%). China (17.2%) remains the second most popular hosting country. In the last six months Spain, which has never appeared in the top 5 listing, has leapt to third place with 15.7% (a 14.5% rise from the first half of the year).

Email Security

- 81% of emails during the second half of the year contained a malicious link.
- Websense Security Labs identified that 85.8% of all emails were spam.
  - Statistics for the second half of 2009 show spam emails broke down as 72% (HTML), 11.2% (image), 14.4% (plain text with URL) and 2.4% (plain text with no URL).
  - Spammers are sending an increased number of blended attacks.
- Tens of thousands of Hotmail, Gmail and Yahoo email accounts were hacked and passwords stolen and posted online which resulted in a marked increase in the number of spam emails.
- Phishing lures have doubled since the first half of the year representing approximately 4% of spam email.
- Websense saw a rising number of shortened URLs in spam messages, a decrease in the use of image spam, and a consistently high number of emails that contained links to URLs.

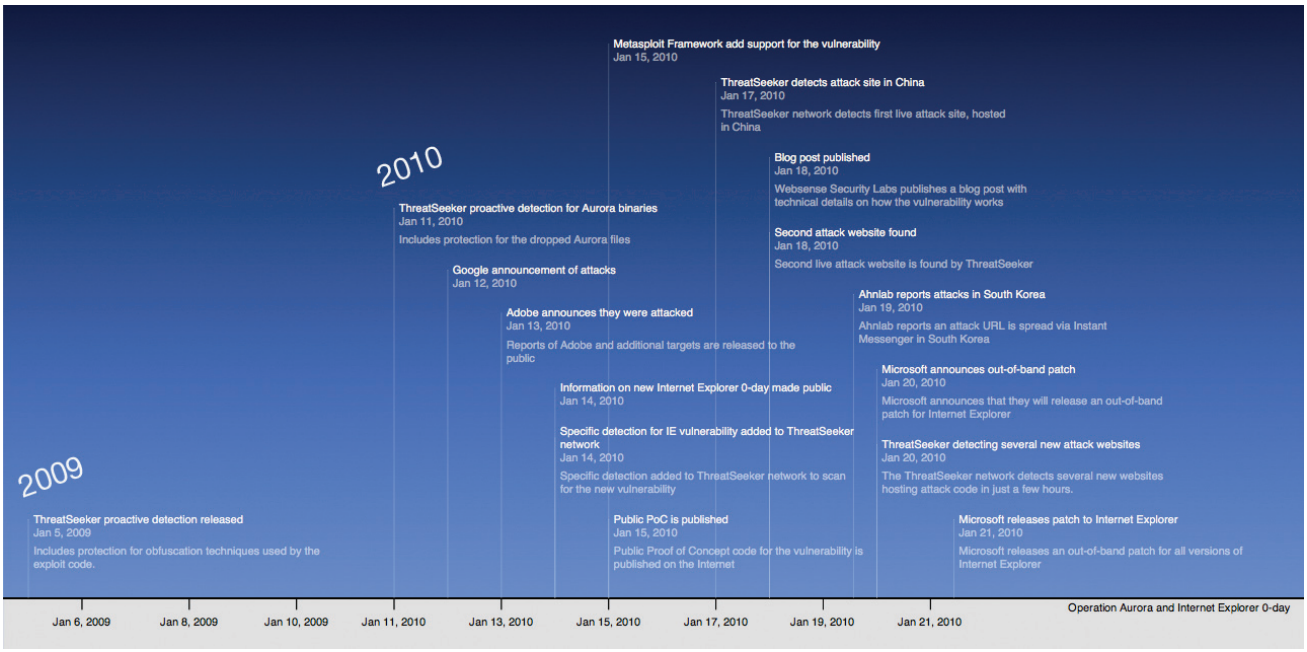
Data Security

- 35% of malicious Web-based attacks included data-stealing code.
- 58% of all data-stealing attacks are conducted over the Web.
- US, Russia, China and Brazil are consistently in the top 5 countries hosting crimeware and receiving stolen data. Canada has moved from number five down to tenth position in the last six months with Germany replacing them in fifth place.

A Look Back at the Last Six Months

Modern, Blended Threats

Modern threats were on the rise, as seen when approximately 30 companies became the victim of a browser-delivered Web exploit targeting sensitive data. The attack, commonly referred to as Aurora, leverages a previously unknown vulnerability within Internet Explorer to access sensitive information from target companies. The vulnerability was discovered in September 2009, but use of the exploit was uncovered in December 2009 and delivered on reputable sites - bypassing legacy anti-virus, URL filtering and reputation technologies and affecting systems operating both inside and outside the corporate network. The nature of this threat – its targeting of specific, enterprise organizations and their sensitive data, its method of delivery – email and the Web, and its make up – a previously unknown browser exploit, is representative of the growing type of modern, blended threats facing organizations today.



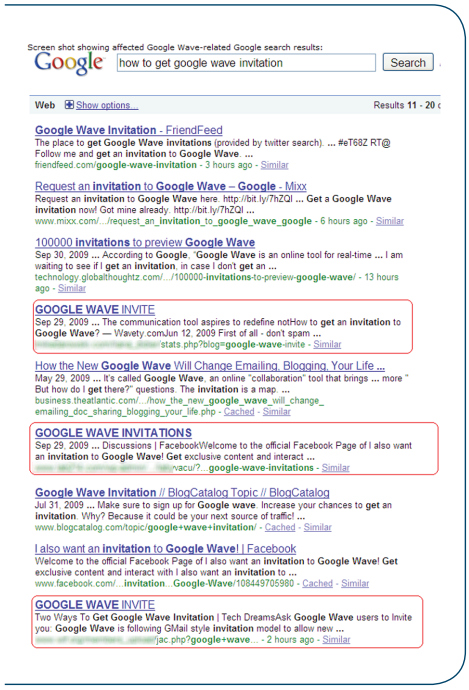
Operation Aurora Timeline

Don't Trust Your Search Results

A malicious search engine optimization (SEO) poisoning attack, also known as a Blackhat SEO attack, occurs when hackers manipulate search engine results to make their links appear higher than legitimate results. As a user searches for related terms, the infected links appear near the top of the search results, generating a greater number of clicks to malicious Web sites.

SEO poisoning has been a popular method of attack for cybercriminals and one that shows they are using more sophisticated techniques. By targeting the top Google searches, hackers are able to drive traffic to sites using highly popular search terms. The average number of malicious sites in any Google search using hot/trending topics (as ranked by Google), by the end of the year, stood at 13.7% for the top 100 results.

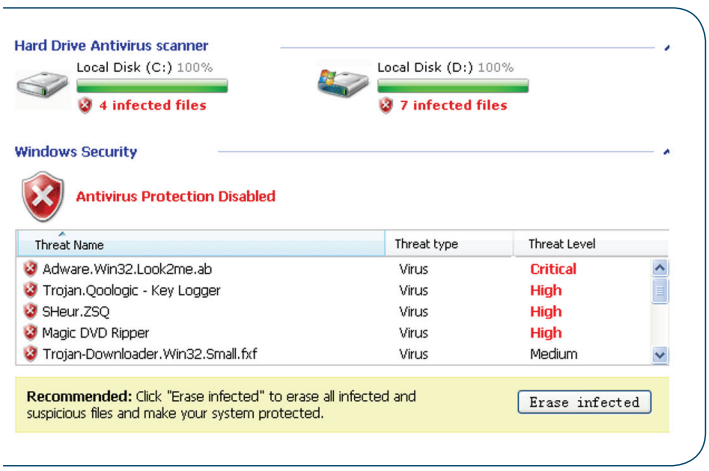
In the last year, attackers have used this technique to poison search results on everything from MTV VMA awards and Google Wave invites, to Labor Day sales. SEO poisoning attacks are successful because as soon as a malicious campaign is recognized and removed from search results, the attackers can automatically redirect their botnets to a new, timely, search term. These ongoing campaigns are likely to gain steam in 2010 and may cause a trust issue in search results among consumers.



Google Wave SEO attack

Rogue AV

The last six months was typified by a growing number of bogus anti-virus campaigns. Users are offered free virus health-checks which 'scan' PC's and claim to find viruses. When the inevitable issue is found, payment is required to enable the 'clean-up'. What the user can't see are the redirections to malicious sites and other exploits happening in the background and by that point they have entrusted their credit card details to cybercriminals. Brittany Murphy's death in December proved a popular target combining SEO poisoning with rogue AV, illustrating a tendency by cybercriminals to pair the attack methods. Websense Security Labs identified that Google top search results on 'Brittany Murphy death' returned links to rogue AV sites.



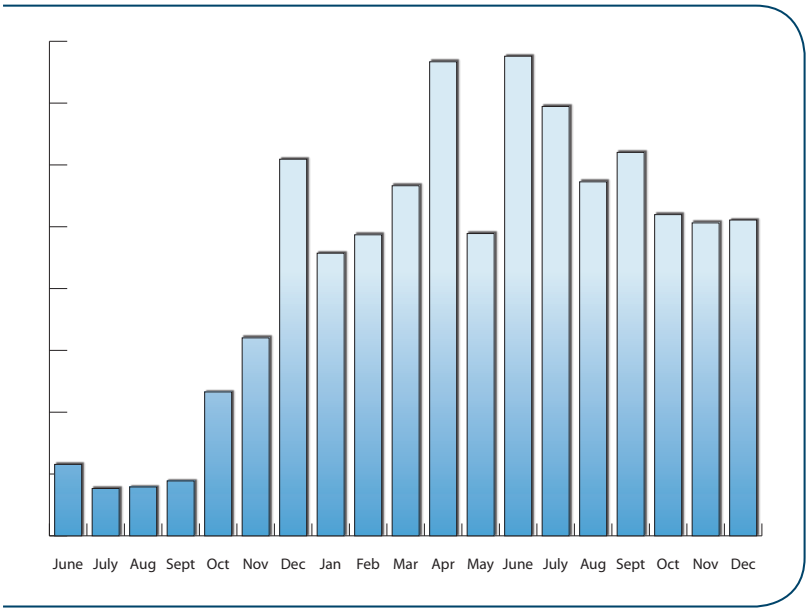
Rogue AV

Capitalizing on Reputation

Malware authors were increasingly targeting legitimate Web sites in the second half of 2009, with 71% of sites with malicious code being existing, legitimate entities. Hackers employ this tactic in order to leverage the trust given to reputable sites. This technique is increasingly popular as a means of bypassing reputation-based security controls. Additionally, existing sites have many returning users (millions in the case of popular consumer, Web 2.0 and social networking sites), all of whom can be harvested for sensitive personal information such as bank account details.

Targeted Attacks

Websense Security Labs has seen a decline in the number of Web sites compromised compared to the first six months of the year. So, while the headline figure might sound promising, it actually means that malware authors are getting smarter about where and how they extend their efforts. The traditional scattergun approach is being replaced by more carefully considered attacks. Hackers have realized that targeting fewer Web sites with higher traffic and multiple pages can be more efficient and effective.



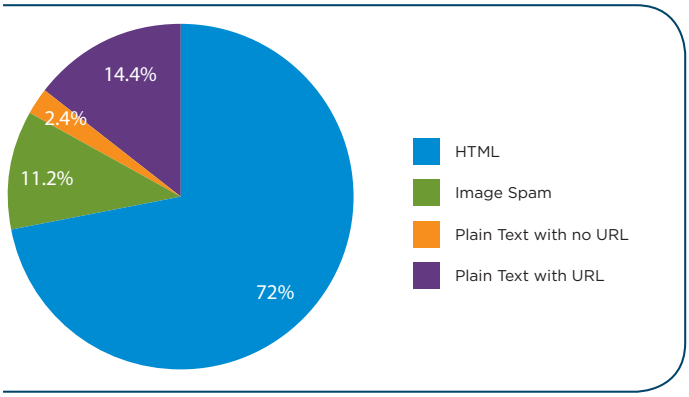
Growth of malicious Web sites over the last 18 months, June 2008 - December 2009

In October a cleverly wrapped social engineering scam used highly customized phishing emails spoofing the popular Microsoft Outlook Web Access (OWA) program. Victims received a message leading to a site to apply mailbox settings which were supposedly changed due to a "security upgrade."

The messages and attack pages are personalized for the email address to imply the message was being sent from tech support of the domain. The URL in the email also looks like it leads to the company's own OWA system. The malicious site was also very believable because the victim's domain was used as a sub-domain to the site so that the attack site appears to be the user's actual OWA site. The victim's domain name and email address are also used in a number of locations on the malicious site to make it appear much more authentic. At one point in this campaign, the ThreatSeeker Network was intercepting these at a rate of 30,000 messages per hour.

Blended Attacks

Blended threats – emails that contain links to spam sites and/or malicious Web sites - remain the most popular vector for spam attacks. Over the year, image spam decreased from 29 percent to 11 percent while plain text dropped from 4 percent to 2 percent.



Spam Types July - December 2009

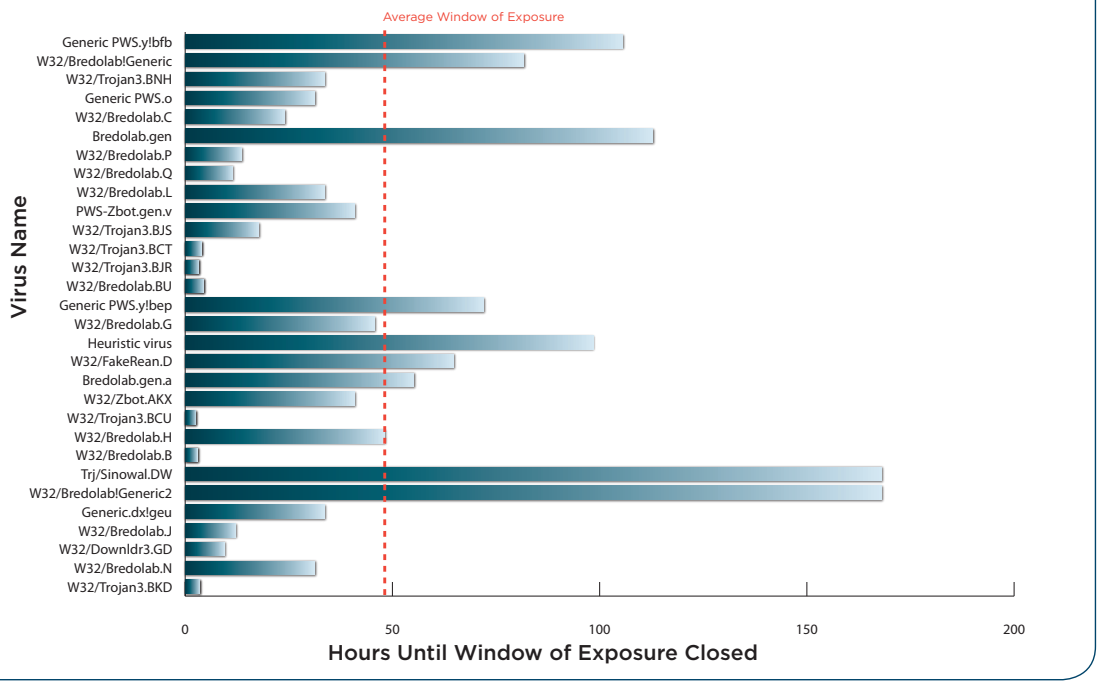
When tens of thousands of Hotmail, Gmail and Yahoo email accounts were compromised in November, Websense Security Labs noted a marked increase in spam.

The hacked accounts were used to send out personalized spam emails to the users contact list – making the recipient think the email had come from a friend or known contact. The spam email recommends a product and invites the reader to click on a link to a shopping site, which was in fact, a fake. Sites were often less than a month old, having quickly shot up the Alexa ranking, indicating that they have seen a lot of traffic. The user then enters a credit card to buy goods, which means the hackers now have the user's bank account details.

This is just another example of online fraudsters becoming increasingly adept at gaining personal and confidential information from unsuspecting victims – this time using email, Web and data elements.

Two days too long

Over the past 6 months, the average time it took for anti-virus vendors to deliver a patch once malware was identified was 46 hours - nearly two whole days - compared to 22 hours in the first six months.



Window of Vulnerability

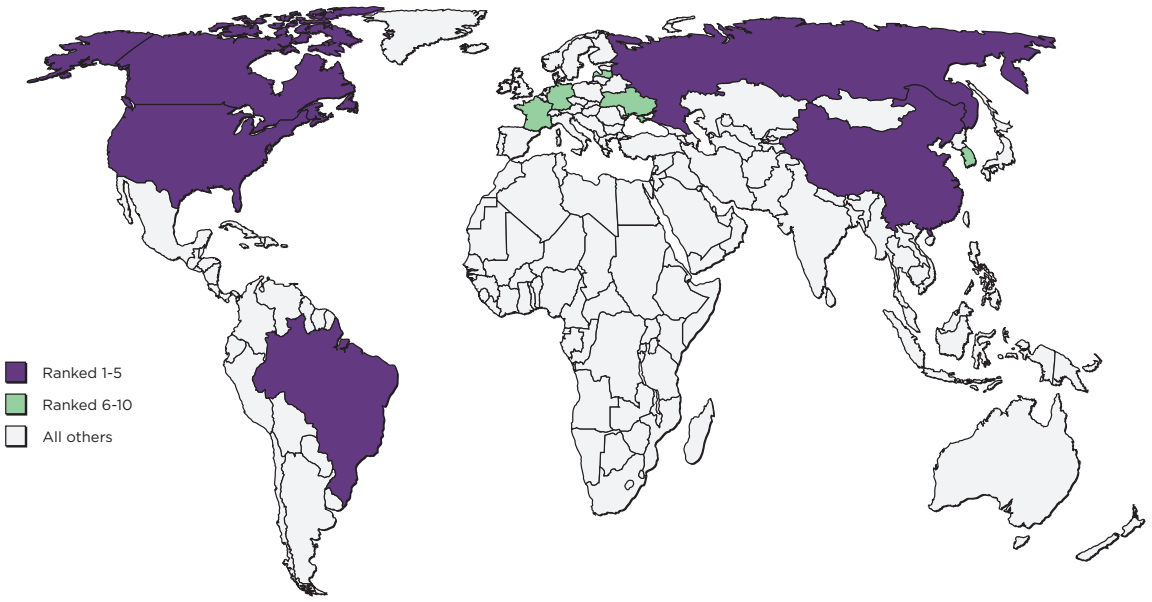
This nearly two day-long window of vulnerability with AV solutions is not fast enough to protect against modern threats. The idea that computer users are not protected for days at a time, or even weeks or a month may be compared with leaving your laptop in a public space for three weeks and hoping it won't be used or abused.

Each day, Websense real-time classification categorized an average of 150 pieces of malware that was missed by all of the top five AV companies. The average classification time for malicious Web sites was less than 2.5 milliseconds with 250,000 new compromised sites classified every day – this greatly contrasts with the two day average window of exposure delivered with AV.

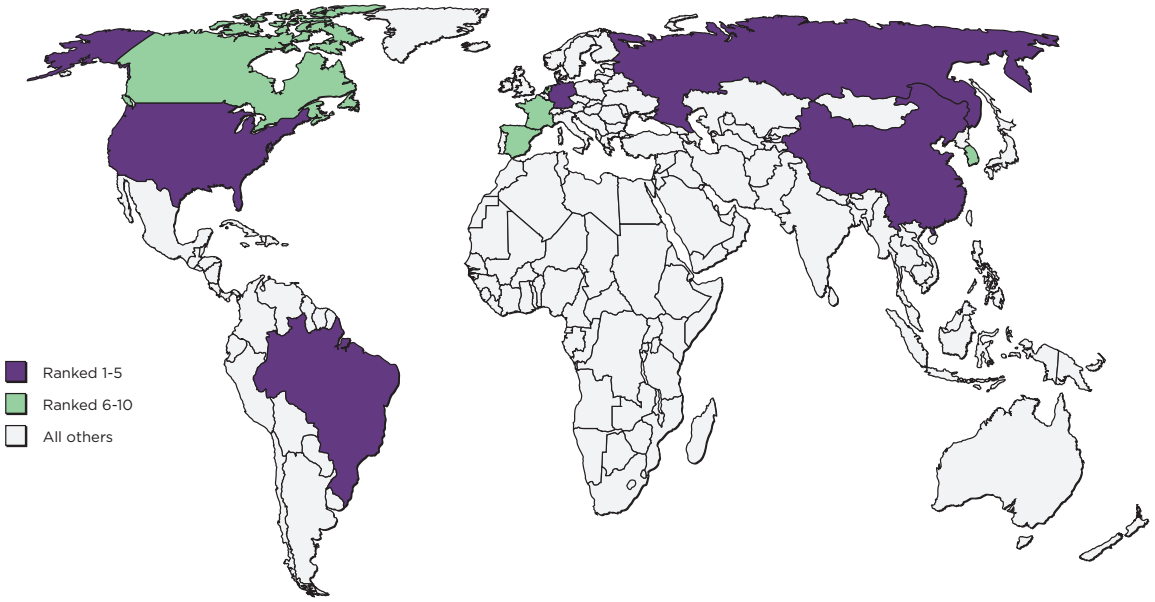
Crimeware across the globe

Crimeware is a class of malware designed specifically to automate cybercrime. Distinct from other kinds of malicious programs such as spyware, adware and malware, crimeware is designed to perpetrate identity theft in order to access the online accounts of computer users for the purpose of stealing money, or exploiting sensitive financial data.

In addition to tracking where stolen data is sent, Websense Security Labs also tracks where crimeware is hosted and, as expected, in the last half of 2009 the United States once again takes the lead.



World map showing top countries hosting crimeware January - June 2009



World map showing top countries hosting crimeware July - December 2009

Follow the Money

September ushered in a new wave of IRS phishing attacks delivered by the Cutwail/Pushdo botnet and serving a ZBot variant. But the most interesting development that month was the emergence of a phishing attack that launches a live chat support window, apparently from the victim's bank, to steal information.

In the UK, phishing attacks purported to be from the Revenue & Customs agency offering tax rebates, but first asking the victim to enter their bank account or credit card details.

One of the top stories to develop in October was the FBI news that cybercriminals are increasingly targeting America's small and medium size businesses with attacks designed to pilfer money out of business banking accounts. The scams all work in the same basic way – the criminals send targeted spear phishing spam emails to individuals in the organization who have access to the company's online banking credentials. They trick them into downloading a Trojan or clicking on a link in the email that leads to a Web site with malicious, data-stealing code. Once the cybercriminals have access to the organizations' online banking credentials they transfer money to "money mules" who have been recruited to forward the funds via wire to the criminals themselves.

The FBI says this mix of banking Trojans and phishing attacks led to $100 million in attempted losses as of October, with actual losses around $40 million.

While the FBI announced indictments of 100 people in the U.S. and Egypt in the largest cybercrime investigation to date in the U.S. - the simple fact is this type of fraud is only going to escalate. As they are blended threats that span Web and email attack vectors in order to steal confidential data, the only way for organizations to protect themselves is through a unified security platform that integrates email, Web and data security functions.

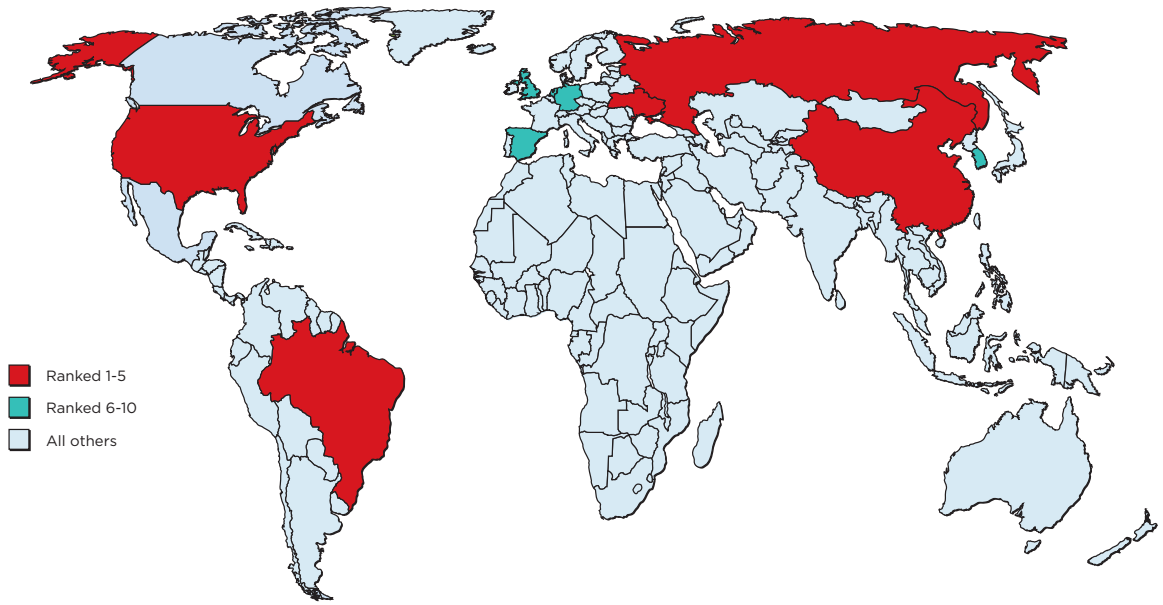
Anniversary of Conficker

2009 was dominated by the Conficker worm. Websense Security Labs saw many unique variants and the worm's spreading capabilities were highly aggressive and powerful – combining online and offline spreading. The worm also populated using USB devices and network shares which meant many users got re-infected even when a patch had been installed.

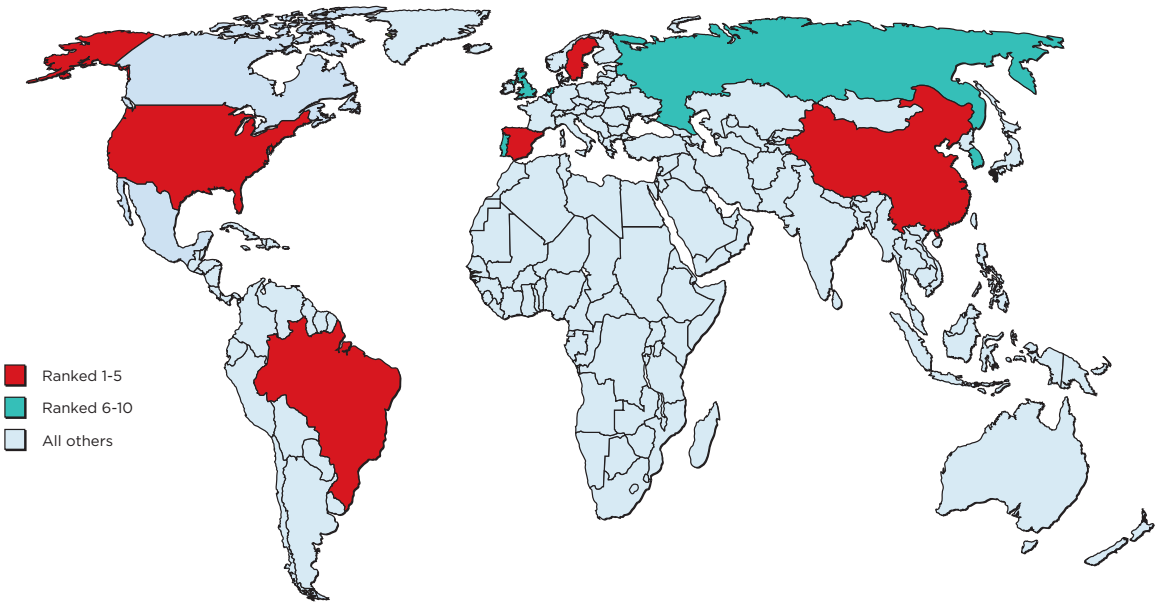
Amongst enterprise and corporate users, Conficker quietened down in the second half of the year as patches were successfully implemented and Autorun from USB devices were disabled. However, there are still 5 million infected computers out there and it is believed they are located primarily in China, Russia & Brazil.

Changes in the Threat Webscape

With data-stealing Web and email attacks on the rise, Websense Security Labs is tracking malware across the world as cybercriminals demonstrate that this is a global concern.



World map showing top countries hosting malware January - June 2009



World map showing top countries hosting malware July - December 2009

Consistent with previous reporting periods, over half of all malware connects to the United States. However as other countries' infrastructure improves and attackers continue spreading their hosting locations around the world, over the course of the year Websense Security Labs has seen a shift in the Top 10 countries to which malware connects. Looking back over the year, China remains the second most popular hosting country and Spain has made its first appearance in the top 5 listing.

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.

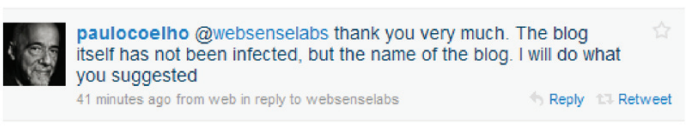
Websense Security Labs alerts

The following are highlights of some of the major attacks discovered by Websense Security Labs during the second half of 2009.

For more details, visit http://securitylabs.websense.com/

Prominent Author's Web site Compromised

Attack Date: 12/04/2009
Attack Details: Websense Security Labs found that writer and blogger Paulo Coelho's blog had been hijacked, compromised, and defaced so that it was advertising Valium. The author was contacted (see Websense Security Labs twitter feed) and the site was quickly cleaned up, however the spam was there long enough for Google to pick it up in within the first 10 search results



Fox Sports Web site Compromised

Attack Date: 12/29/2009
Attack Details: Websense Security Labs ThreatSeeker Network detected that the Fox Sports site had been compromised and injected with malicious code. Fox Sports is a division of the Fox Broadcasting Company. It specializes in the latest sports news and world sports updates. Fox Sports has an Alexa ranking of 330.

Operation Aurora and Internet Explorer Zero-day

Attack Date: began in December 2009
Attack Details: News of targeted attacks on Google, Adobe, and other large companies were made public in early January 2010. Microsoft confirmed that the attacks used a new security vulnerability in Internet Explorer, unlike the majority of targeted attacks which use email attachments sent to recipients at a target organization. The vulnerability in Internet Explorer was similar to other vulnerabilities in that it allows the attacker to perform a drive-by download attack which means that the user only needs to visit a Web site or view a specially crafted HTML email to be infected.

Websense ThreatSeeker network includes protection for obfuscation techniques used by the exploit code since early January 2009 and therefore was able to protect customers against this vulnerability even before it was discovered. Websense Security Labs analyzed the code and worked with Microsoft to identify Web pages using the new vulnerability.

The next 12 months

The emerging trends and predictions by researchers in the Websense Security Labs point towards increasingly blended security threats attempting to rope computers into bot networks and steal valuable confidential information. Specifically, hackers will look to compromise new platforms such as smart phones, take advantage of the popularity of Windows 7, compromise the integrity of search engine results and use legitimate advertisements to spread their malicious content. At the same time, malicious attackers are increasing the number of traditional attacks on PCs, with quickly changing tactics and new twists on old exploits.

In the coming year, there will be even more spam and attacks on the social Web and real-time search engines such as Topsy.com, Google and Bing.com, which recently added real-time search capabilities. The trend, set to continue this year, began in 2009 with increased malicious use of social networks and collaboration tools such as Facebook, Twitter, MySpace and Google Wave to spread attackers' wares. The use of Web 2.0 sites by spammers and hackers has been successful because of the trust users place in the platforms and the other users.

Last year, Websense Security Labs saw an increase in botnet groups using similar spam/Web campaigns tactics such as fake DHL and USPS notifications and we expect this to continue in 2010. We also anticipate more aggressive behaviour between botnet groups including bots able to detect and actively uninstall competitor bots.

In 2010, emails - often using popular topics - will re-emerge as a key medium for spreading files and delivering Trojans as attachments following an upsurge last year. Researchers have also seen increasingly sophisticated blended attacks that are difficult to close down, as well as simple malicious data stealing attachments and URLs.

And as take-up of Windows 7 ramps up after its October launch, we expect to see more malicious attacks with specific tricks to bypass User Access Control warnings, and greater exploitation of Internet Explorer 8.

SEO poisoning attacks are successful because as soon as a malicious campaign is recognized and removed from search results, the attackers can automatically redirect their botnets to a new, timely search term. These ongoing campaigns are likely to gain steam in 2010 and may cause a trust issue in search results among consumers, unless the search providers change the way they document and present links.

We will also see a major ramping up of efforts to target smart phones such as the iPhone and Android. Essentially miniature PCs, they will face the same types of dedicated attacks as computers after the first major attacks on the iPhone were documented at the end of 2009. The poor security of applications on smart phones, used increasingly for business and conducting financial transactions, will make the devices even more vulnerable.

In a high-profile incident in 2009, visitors to the New York Times Web site saw a pop-up box warning them of a virus that directed them to an offer for antivirus software, which was actually rogue AV. The pop-up was legitimately bought advertising space, something we expect to see a lot more of this year.

During 2009, Apple released six large security updates for Macs, a clear indication of the potential for attacks aimed at OS X. We expect there to be even more security updates as hackers ramp up attacks targeting the increasingly popular platform across both consumer and business markets. There is also the potential for the first drive-by malware created to target Apple's Safari browser.

The blended nature of today's threats means that all security measures must integrate email, Web and data policies. Websense anticipates, discovers and mitigates these evolving threats as a central part of our technology strategy, and integrates that content and threat knowledge into a unified Web, email and data loss prevention solution.

Sign Up for Free Websense Security Labs Alerts

Websense® Security Labs™ discovers and investigates today's advanced Internet threats and publishes its findings. Websense Security Labs alerts enable organizations to protect employee computing environments from increasingly sophisticated and dangerous Internet threats. In addition to posting alerts to this website, Websense Security Labs alerts are now available through email.

To have the latest security warnings on malicious internet events, including spyware, phishing and corrupted Web sites, sent directly to your inbox as they are discovered by Websense Security Labs, simply provide your email below. If you are already subscribed and wish to unsubscribe from these alerts, please click here.

Say Yes to Essential Information Protection

Websense integrates Web security, email security, and data security to protect essential information and enable productive, safe use of the Internet platform. Websense Essential Information Protection software defends cross-channel communications, safeguards Web 2.0 use, and prevents data loss. Essential Information Protection uses the ThreatSeeker Network, an advanced infrastructure for early threat discovery across email and Web channels, real-time identification and blocking of high-risk Web sites, and data identification techniques and technologies. Websense Web, email, and data security solutions use security intelligence from the ThreatSeeker Network to provide the most up-to-date information protection from data loss, unwanted content, and malicious threats.

To find out how Websense provides the best security against modern threats at the lowest total cost of ownership, visit www.websense.com.

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.

websense®
ESSENTIAL INFORMATION PROTECTION™