

2010 Threat Report

A Websense[®] White Paper

CONTENTS

- Introduction 3
- Websense® Threatseeker® Network Research Highlights, 2010 4
- Overview 4
- Key Statistical Findings 4
 - Web Security
 - Email Security
 - Data Security
- Significant Events In 2010 6
- Malware: Tricks And Treachery 8
- Web Woes 14
- Email Enticements 15
- Data Dangers 19
- Social Networking: The Big Picture, The Big Risks 20
- Websense Security Labs™: Major 2010 Discoveries 25
- The Next 12 Months 28
- Summary 29

INTRODUCTION

Websense® Security Labs™ uses the 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 1 billion pieces of content daily, searching for security threats.

Every hour the ThreatSeeker Network scans more than 40 million websites for malicious code and nearly 10 million emails for unwanted content and malicious code. Using more than 50 million real-time data collecting systems, it monitors and classifies Web, email, and data content. Together with the Websense Advanced Classification Engine — an advanced composite content classification engine embedded in Websense solutions — the ThreatSeeker Network provides 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 2010.

WEBSense THREATSEEKER NETWORK RESEARCH HIGHLIGHTS, 2010

Overview

The Web landscape continued to evolve during 2010. The most visited websites pulled away from the pack in their content and functionality with the majority having a more socially dynamic presence. In 2010, hackers adapted their strategies to address the social and dynamic Web. Attacks became more blended, sophisticated, and targeted. Many of these attacks used new tricks and methods of delivery. Script-based attacks, blended email campaigns, and search engine optimization (SEO) poisoning were all common. Even the most easily detected threats and botnets were successfully repurposed. The majority of attacks in 2010 focused on the same thing: stealing data.

“Searchers beware!” could have been the new motto as hackers spent a lot of time compromising legitimate websites. News headlines and entertainment buzz continued to be a choice target for SEO attacks. Rogue antivirus (AV) combined with SEO poisoning was a commonly used technique. Email attacks were successfully repurposed with HTML and PDF files, whereas traditional phishing attacks became a little easier to recognize.

2010 saw not only continued sophistication on the part of cybercriminals but also a tightening of the organizational structures in which they operate. Turf wars between cybercriminal organizations will continue to develop in what has literally turned into a fully operational underground economy.

Key Statistical Findings

Web Security

- Websense Security Labs identified a 111.4% increase in the number of malicious websites from 2009 to 2010.
- 79.9% of websites with malicious code were legitimate sites that have been compromised— an increase of 3% from the last previous period.
- Searching for breaking trends and current news represented a higher risk (22.4%) than searching for objectionable content (21.8%).
- The United States was the top country hosting phishing sites in 2010.

Email Security

- 84.3% of email messages were spam — a 0.7% decrease over last year.
- 89.9% of all unwanted emails in circulation during this period contained links to spam sites or malicious websites — an increase of 4% over 2009.
- Shopping remained the leading topic of spam (12%), although it dropped by 13%. This correlates nicely with economic consumer spending trends, since the recession caused some shoppers to ease back on spending.

79.9% of websites with malicious code were legitimate sites that have been compromised.

84.3% of email messages were spam.

52% of data stealing attacks occurred over the Web.

- Pump and dump (10%) and education-related (9%) spam emails were also popular. Pump and dump spam is intended to get victims to buy stocks to artificially drive up the stock price, making a neat profit for the spammers who bought the stock at a low price.
- 9% of data stealing attacks happened over email.

Data Security

- The United States was the #1 country where malware connected on the Web.
- pc-optimizer.com was the #1 host of data stealing code in 2010.
- 52% of data stealing attacks occurred over the Web.
- Concerns about accidental data loss have become a front burner issue for many organizations in 2010.
- The United States and China continued to be the top two countries hosting crimeware and receiving stolen data during 2010. The Netherlands has found its way into the top five.

SIGNIFICANT EVENTS IN 2010

Stuxnet - Physical Attack 1.0

“Stuxnet has the same surgical capabilities as a stealth bomber.”

Ali Mesdaq, Websense Security Researcher

Most modern threats are geared towards financial gain. During June 2010, the world witnessed what is considered to be the first major attack specifically designed to go after Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems are designed to control and monitor various processes within industrial systems. The Windows-specific worm used various zero-day attacks to target Siemens's WinCC/PCS 7 SCADA software. It spread via infected USB flash drives then used other exploits to go after network-based WinCC computers. After getting inside the system, it used default passwords to command the software.

What made Stuxnet so different than the other attacks during 2010 was the level of sophistication, the fact that it specifically targeted critical infrastructure and the geo-specific location of the event. Many of the attacks were aimed at facilities in Iran. Although the attack surfaced in other countries, there were a large portion of attacks that happened at key nuclear facilities in Iran. The surgical precision of the attacks was stellar and the attack locations have drawn speculation about the identities of those behind the attack.

Zeus Arrests - 20-Year-Old Uses a Notebook Computer to Steal 20 Million Bucks and a Paper Notebook to Count the Cash

Nineteen Eastern Europeans were arrested in September for raking in \$3 million per month with help from Zeus, a Trojan Horse designed to steal banking information. The group used Zeus to quietly infiltrate computers with weak security systems. Once inside, it would wait for victims to log into a variety of specifically targeted banks. The users credentials were stolen and forwarded to the group's criminally controlled server. This criminal organization also used Zeus to manipulate Web browsing sessions where Zeus would prompt users to give up additional sensitive information.

London police estimated that over 600 accounts were hacked into, resulting in a loss of around \$20 million. The leader of the organization was 20 years old and ran most of the operation from a laptop in his three-bedroom U.K. apartment. He used a paper notebook and a pencil to count the money.

Operation Aurora - The Modern Email, Web, and Data Threat

News of targeted Chinese-based attacks at numerous companies came out during December 2009 and January 2010. Targets included Adobe, Google, Rackspace, Northrop Grumman, Dow Chemical, and governments in Germany and France. The initial assumption was that the attacks were done with malicious PDF files until Microsoft released information that they were done with a new security vulnerability in Internet Explorer ([CVE-2010-0249](#)). Up until this point most targeted attacks had typically included email attachments (e.g., PDF, Microsoft Word, Excel, or PowerPoint files) that would be sent to individuals at specific organizations. The vulnerability in Internet Explorer was very similar to other vulnerabilities we have seen in Microsoft's browser in that it allowed the attacker to do a drive-by download. This means that a user's system can be compromised simply by visiting a website or viewing a specially crafted HTML email. The Aurora attack highlights how it could be just a matter of time before we see additional large-scale attacks using the new vulnerability.

Equally alarming is the fact that this attack revealed how many organizations are still using a browser as old as Explorer 6.0. We examined our own website visitor statistics for websense.com and the results were quite surprising. It turns out that Internet Explorer 6.0 is the second most popular browser representing 19.6 percent of all visits.

WordPress Attacks – The World’s Biggest Blogging Platform Keeps Getting Hacked

Blog platforms have always been vulnerable to attacks. And our research shows that 56 percent of all compromised blogs are attacked more than once. WordPress (used by more than 13.9 million blogs), the world’s most commonly used blogging software platform, was hacked numerous times throughout 2010. Although WordPress releases new versions approximately three times per year, our research shows that many people are using much older versions of the software. Numerous vulnerabilities were known to exist during the height of the attacks. GoDaddy (Hosts 43 million domains and other hosting sites) saw persistent attacks in 2010. Something else worth noting is that when celebrity blogs are hacked, many people assume this means public defacement or an attempt to defame celebrity status. Although this happens on occasion, most attacks target financial gain.

Massachusetts Hospital Loses 800,000 Data Files

In July, Massachusetts-based South Shore hospital publicly announced the loss of 800,000 files that included 15 years of health and financial information of patients, business partners, vendors, staff, and volunteers. The variety of information lost varied from person to person but included the following: full name, address, phone number, date of birth, Social Security number, driver’s license number, medical record number, patient number, bank account information, credit card number, and medical diagnoses and treatment records. After investigating the incident, the hospital chose not to reach out to any of the individuals potentially affected by the breach. The Massachusetts Attorney General’s Office objected to the hospital’s decision, maintaining that affected consumers should receive individual notification concerning the data loss. The Attorney General’s Office continues to monitor and investigate the hospital’s actions as regards the data breach and its response.

Hackers Exposed over 100,000 AT&T Customers iPad Records

In June, a cybercriminal organization named “Goatse” was able to exploit a security flaw through an AT&T Web application. The breach exposed email addresses of iPad 3G users. Many high-ranking media, as well as government and military members of Apple’s early adopter program, were on the list. Numerous members of the U.S. Department of Defense’s advanced research team had their information exposed. Websense believes that Apple will continue to be a choice attack target, as the consumerization of their products quickly flourish in many work environments.

MALWARE: TRICKS AND TREACHERY

“Greed is only limited by one’s imagination. The security decision makers of today need to understand what this means or they will lose.”

Stephan Chenette, Websense Security Researcher.

In 2010, the end goal for malware authors remained making money. The increasing sophistication of their schemes has changed the threat landscape so significantly that most people don’t really understand what they are trying to defend against. Machines and networks are no longer the core focus of malware authors. USB sticks and social networks are all heavily abused mechanisms used to reach financial gain. The dynamic nature of the Web compared to what is being served up on a geographical basis changes every hour.

One of the biggest misunderstandings is that antivirus protection is sufficient. But our research re-affirms that today’s attackers routinely pre-test their malware against the top AV solutions. Although AV is a necessary tool, signatures have simply become a subset of a much bigger problem. Real-time security has become the focus of the modern hacker.

Our statistics show that 22.4 percent of real-time search results on entertainment will lead to a malicious link.

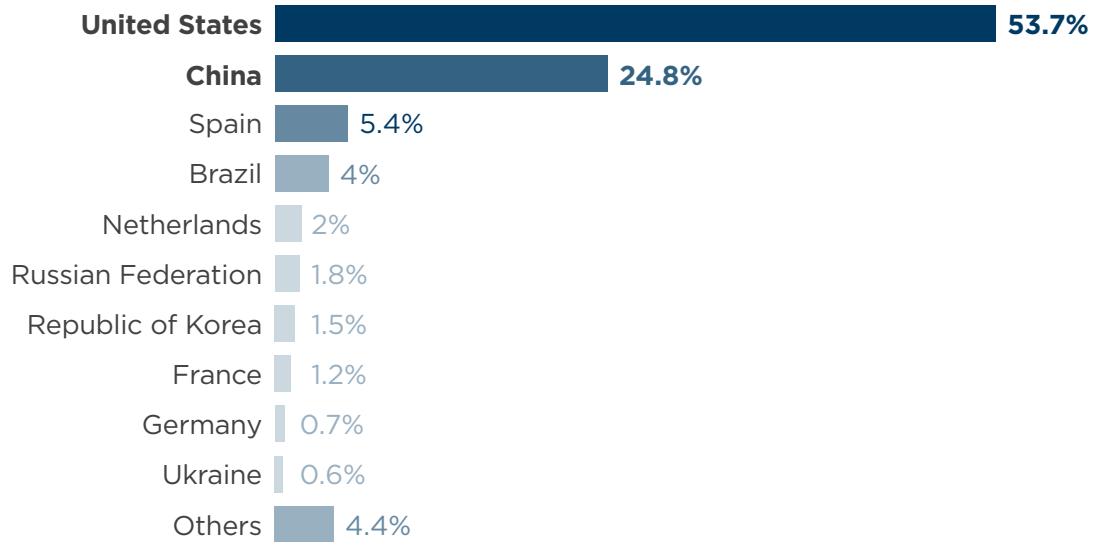
The shark swims where the seal plays. SEO poisoning continued to be one of the most significant trends throughout 2010, as malware authors focused on entertainment buzz and breaking news. The earthquakes in Haiti and Chile, Corey Haim’s death, and the World Cup of Soccer were just a few examples of cleverly manipulated search engine results steering people to bogus links that rated higher than legitimate results. Similar to what we found in 2009, the botnets behind these campaigns are being repurposed once the illegitimate campaign has been removed from the search engine results.

Many of the 2010 SEO attacks were blended in nature, with a second component consisting of Rogue AV (another trend we saw last year). Both approaches used bogus AV campaigns offering free health scans that identified fake infections. Upon notification of a fake virus, users were prompted to download a free “antivirus” software where a second scan asked them for their credit card information to remove the fake malware.

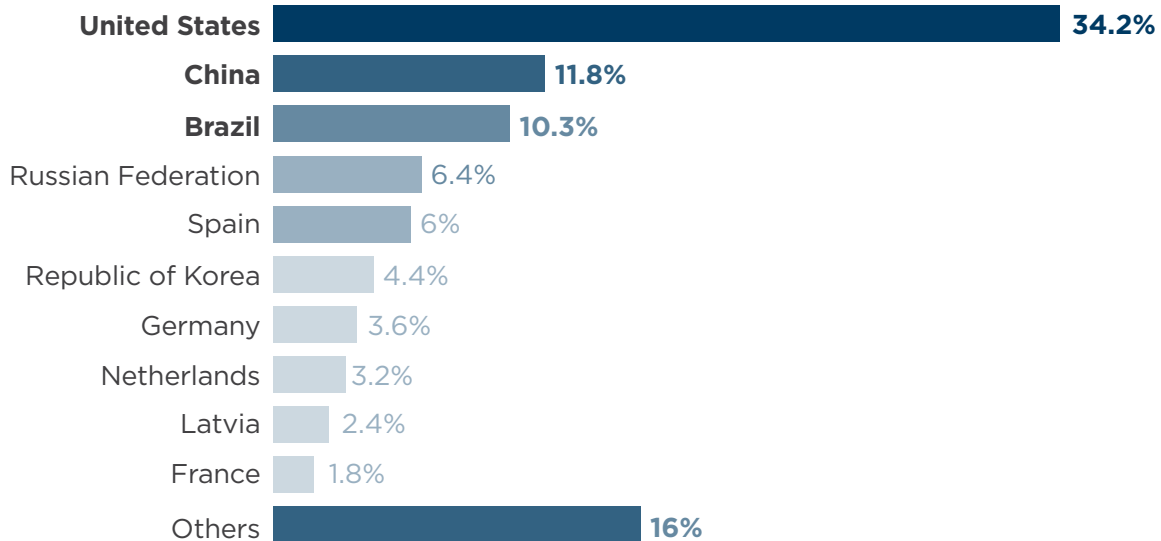
In February, we discovered a new twist in certain attacks. Many tainted SEO results appeared to have PDF files in the link results. This attempt proved to be successful as many people saw this as a form of authenticity.

Our statistics show that 22.4 percent of real-time search results on entertainment will lead to a malicious link.

Top 10 Countries Where Malware Connects on the Web in 2010



Top 10 Countries Hosting Crimeware* on the Web in 2010



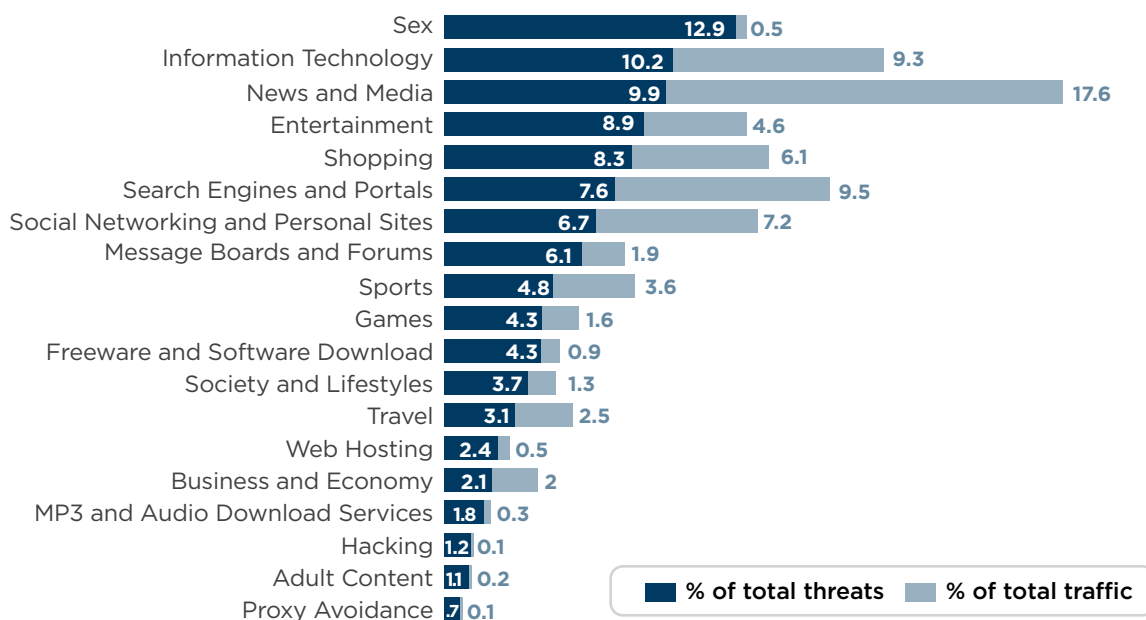
*Crimeware is a type of malware specifically used to conduct cybercrime.

The road to malware through link analysis

Computer users do not deliberately visit infected websites, therefore a cyber criminal needs some sort of hook or incentive to encourage a user to visit an infected site. This is often referred to as the “social engineering” element of cyber crime. Here we outline what sort of user behavior patterns are likely to lead to exposure to malicious software, based on our analysis of data in 2010.

Websense has the capability to scan any page for malicious links. This technology was used to analyze traffic from the Websense Hosted Web Service. Web pages that contain malicious links may not deliver threats themselves but the existence of malicious links means the user is one click away from a malicious site.

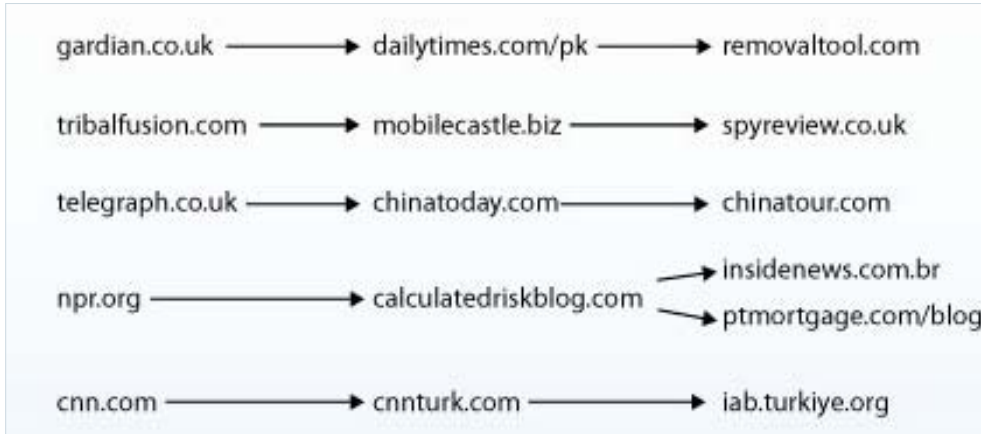
The following graphic shows the number of visited pages containing malicious links for a sample of hosted Web traffic pulled during 2010.



Sexually explicit content has always posed a risk to organizations. For the average company the single biggest exposure to malicious content comes from access to sexually explicit content. This is the case even when it represents a tiny percentage of the total content visited.

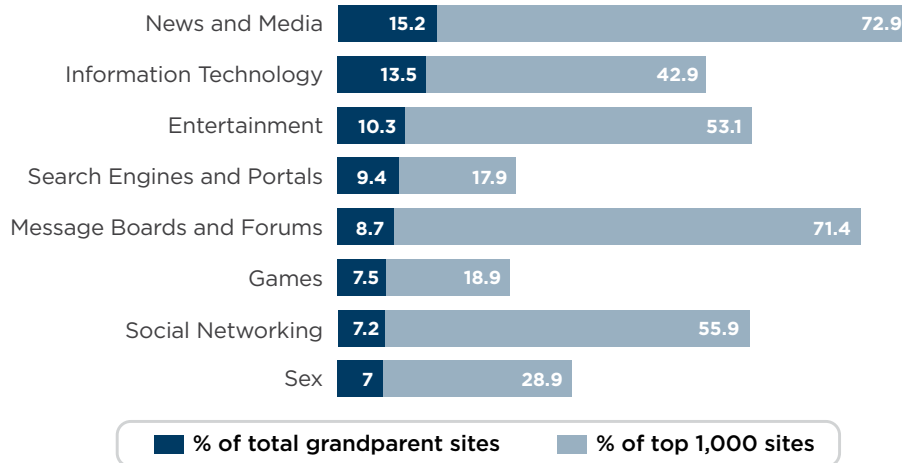
Exposure to sites that contain infected links means that users are one click away from infection (parent sites). In order to characterize sites that were two clicks from infection, we examined the Google search engine to identify sites that linked to these parent sites (grandparent sites).

The graphic below shows examples of how just two clicks can lead from safety to danger.



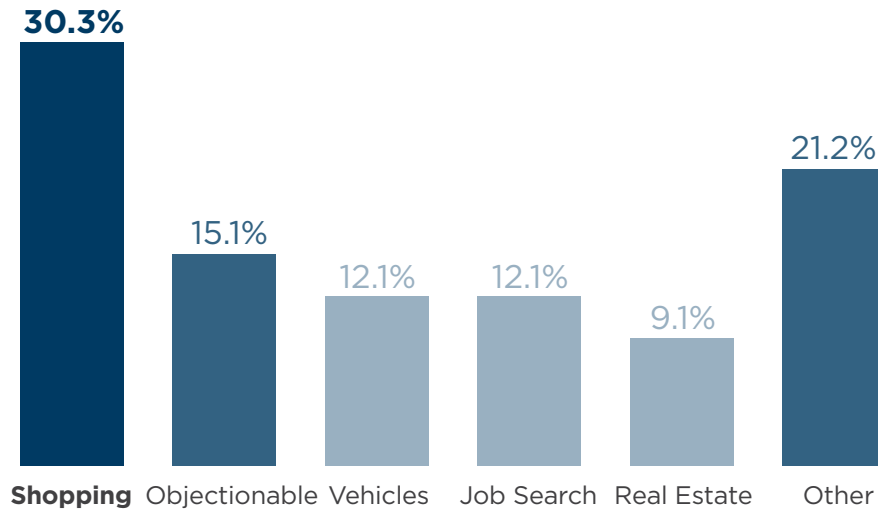
The sites containing spyware were infected at the time of research. They may no longer be infected.

The graphic below shows the category breakdown of the grandparent sites and the percentage of Alexa top 1,000 sites that were identified as being two clicks from malware.



These results show how the path to malware often starts in the recreational Web. They also show that the majority of high-ranking sites are perilously close to danger.

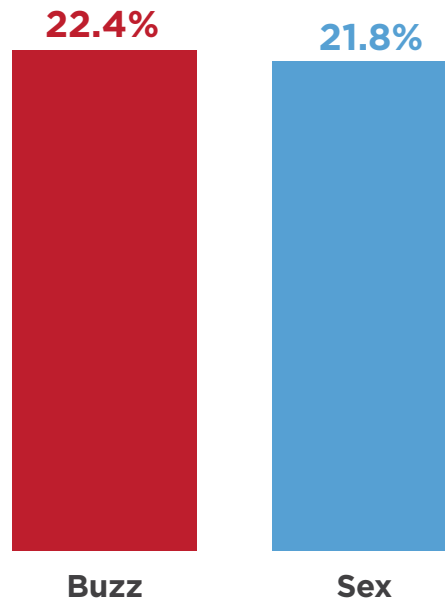
Websense provides the Websense ThreatSeeker® Cloud, which extends Websense content security technology and our global Security-as-a-Service (SaaS) infrastructure to third parties allowing them to integrate URL security analysis into their products. The ThreatSeeker Cloud constantly monitors content for threats. The graphic below shows how we analyzed the data to identify the main category of sites in Google searches that returned malicious sites.



As you can see, non-work-related searching (e.g., shopping, vehicles, job search) represents the biggest risk to spyware exposure. Business and Information Technology-related searches did not represent a significant risk.

Non-work-related searching represents the biggest risk to spyware exposure.

In order to investigate this further, infection rates were measured for sets of search terms encompassing known sex terms, popular trending terms from Google and Yahoo and popular business search terms from bnet.com. The percentage of infected searches is shown below:



These results demonstrate that breaking trends represent a risk that is even higher than objectionable content. What was particularly worrisome is that some breaking trends such as “World cup 2014” and “ABS-CBN News” returned searches where more than 25 percent of the sites hosted malware.

No form of Internet usage is completely safe. Even legitimate access to content essential for one’s job function can expose the network to threats. This data is not hidden away in the dark corners of the Web but is accessible within a few clicks of the most prominent sites.

The results above have shown that denying access to objectionable content can greatly reduce exposure to malicious sites. There is also a big risk from non-productive Web usage. The dangerous nature of sites on the bleeding edge of the Internet means that on-premise protection using content inspection offers significant benefit over signature-based protection.

Breaking trends represent a risk that is even higher than objectionable content.

WEB WOES

“What should organizations be most afraid of? You no longer have to go to dark corners of the Internet to find bad stuff.”

Patrik Runald, Websense Security Researcher

In 2010, the Web continued to be the biggest path to malware. There seems to be no shortage of ill-intended, cleverly crafted websites designed to serve up the worst kind of trouble. Malware authors are also working the other side of the fence, as they secretly host their wares on very popular legitimate websites. No longer do people have to go to dark corners of the Internet to encounter threats. Though many Web surfers believe they can let their guard down when visiting more reputable sites, SQL injections and malvertising (malicious advertising) were found on such sites as The New York Times, Gizmodo, and TechCrunch.

Even the most common searches were littered with poison. Google is considered by many organizations as one of the safest places their employees can turn to for information. However, users are now being attacked much more often on search engines.

Web image results have always shown a strong connection between malicious and adult material. Our 2010 analysis of Bing Adult image and video queries shows that 8.18 percent will result in a search results page that contains a malicious link. Our research results on Google adult image queries were even more striking. We found that 50.38 percent of queries will give us a search results page that contains a malicious link. Our analysis shows that once you step into the land of objectionable content, you are heading down the road to even worse content.

How likely it is that searching for trending news and buzz words will lead to malware in 2010? **22.4%**

Percentage growth of malicious sites: **111.4% increase from 2009 to 2010**

What percentage of the top 100 most popular websites are categorized as Social Networking or search? **65% of Top 100 and 95% of Top 20**

Percentage of websites found with malicious code that are compromised legitimate sites versus sites purposefully set up. **Total = 79.9%** (pretty steady)

EMAIL ENTICEMENTS

“Email brings the problem to your doorstep and 75% of the time AV will let it in for dinner. This is why more advanced security analytics are required than just signatures.”

Jon Crotty, Websense Research Marketing Manager

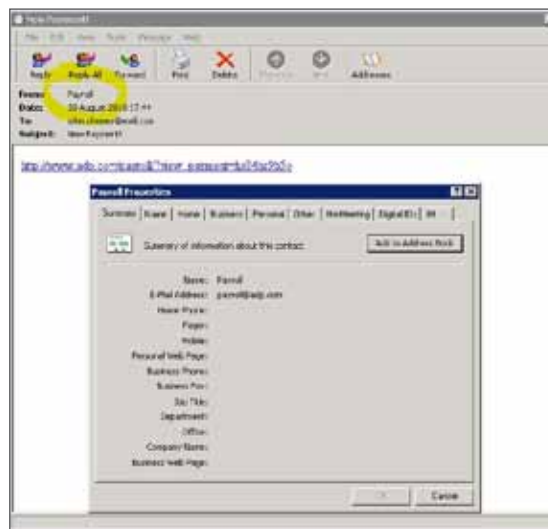
Like other threat vectors, the core focus of email attacks has always been the same: Get in any way you can and extract as much as you can. We found that while the creativity surrounding email and blended threats slowed at the beginning of the year, the new waves of blended attacks are successfully incorporating email as a point of entry. We also saw a continuous flow of new tricks and techniques being used. Midway through 2010 it got to the point where some of the savviest recipients couldn't decipher between good and bad emails.

Reputation services have simply become ineffective as email plays one role in the grand scheme of larger blended attacks that also have Web and data components. Hackers use the dynamic nature of the Web to craft these attacks in real time.

The quantifiable metrics haven't changed too much from a historical perspective. Things such as the amount of spam sent, geographic deployment volume, and emails with malicious links typically see consistent single-digit positive or negative growth or both. Occasionally there is a spike in the numbers, but for the most part these trends move up and down at a somewhat predictable pace. The more erratic component of email security is the micro trending within these categories. The rate in which hackers are repurposing their email campaigns has become staggering.

Criminal malware and email authors place a lot of focus on the same news events and trends. One could say that they operate at a speed faster than real time because they have the ability to plan surgical attacks based on the calendar year. There was nothing stopping criminal organizations from planning blended World Cup spam campaigns (World Cup Blog) months in advance. Unless Patch Tuesday (Patch Tuesday Scam Blog) moves to a Friday and Tax Season starts (Tax Season Scam Blog) in the summer, the likelihood of these types of threats diminishing in volume and potency is slim.

Cleverly crafted payroll and shipping scams involving companies such as ADP, FedEx, and UPS were quite prevalent during 2010. Amazon.com and Buy.com were also used as fronts in very successful spam campaigns.



Email threats used for brand jacking in 2010 proved that many organizations without proper unified content security solutions that provide Web, email, and data security technologies are sitting targets. There were numerous mass emails fronting to be from large brand name companies such as IKEA, Macy's, Best Buy, Target, and Evite. The campaigns used a blended approach by offering the same rogue AV strategy that was often used in previous attacks. On average, only one of every four AV companies detected the big brand name threats.

After a very short period of hiding out, Gumblar was back in full force doing an impersonation of Amazon.com. The aim of the campaign was to trick unsuspecting users to visit a client-side exploit-serving URL.

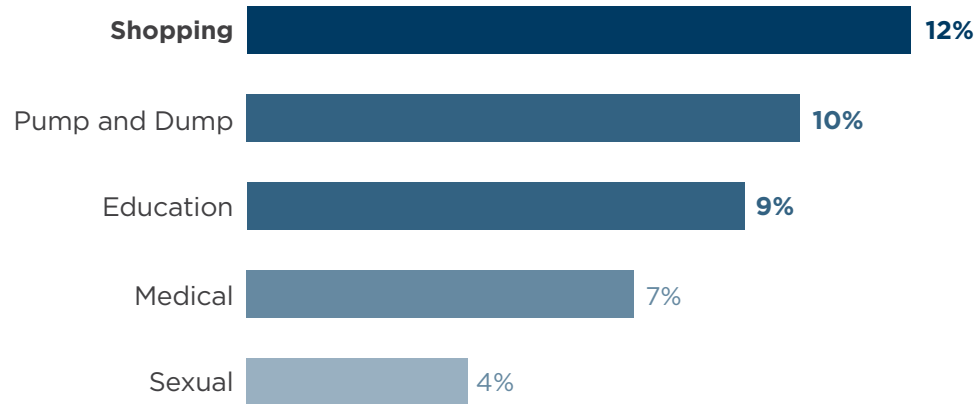
Just like some of the 2009 campaigns we witnessed, Zeus was very much on the radar. Attackers had used Zeus kits to target government and military personnel in the U.S. and U.K. One campaign pretended to be from the National Intelligence Council. Hackers used it to entice victims into downloading a document about the "2020 project," Another targeted CIA personnel, luring them to download a Windows "update" against an attack. In both cases, victims who fell for the trap found their machines infected with the Zeus malware.

Trojans such as Zeus are sold as crimepacks in underground markets and used by a wide variety of criminal organizations. There are so many variants of Zeus-themed spam being spread around that it simply won't go away. Right around the time when many users figured out the latest link-based email attacks, the hackers started coming back with more stealthy techniques such as leveraging exploited PDF and HTML files. The bodies of these emails and the tricks themselves have become much more aesthetically pleasing and sophisticated.

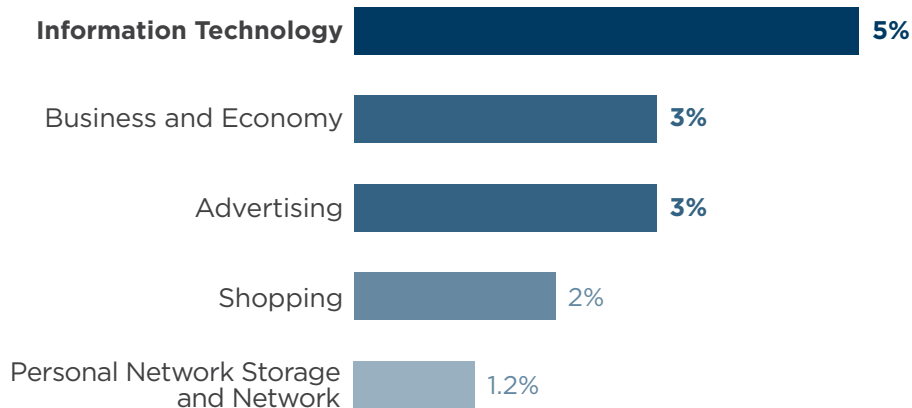


Spam volume during 2010 continued to remain steady at 84.3 percent of all email. This remained fairly steady. In fact, the last two years only saw a 3 percent fluctuation. During 2010, 89.9 percent of all unwanted emails (spam and malicious) contained at least one link. This represented a 3 percent increase over last year.

Percentage of Top Spam Topics by Email Content



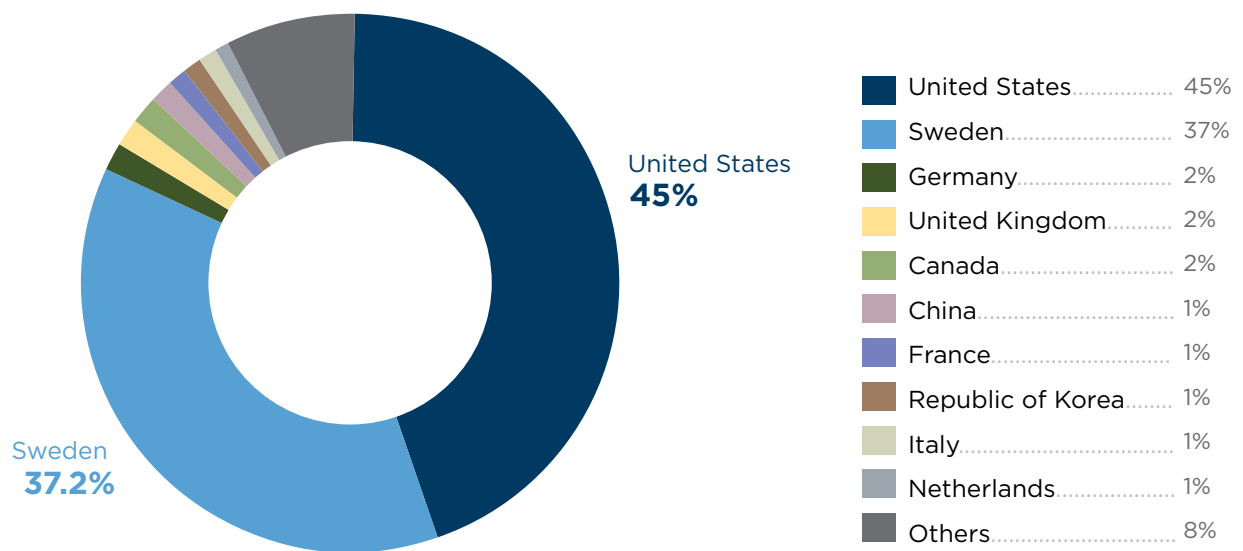
Percentage of Top Spam Topics by URL Category



Pump and Dump spam saw the biggest percentage gain as people were hoping to capitalize on the stock market in an uncertain economic climate. This type of spam typically promises +5 percent gains, but actually provides major losses as the spammers prepare to sell these stocks just after the spam is sent out. Unlike other financially targeted spam techniques (fake lottery winnings and fee transfer scams), the recipient isn't asked to follow up with the sender.

Phishing attacks accumulated making up 0.6 percent of spam messages for email content and 0.1 percent for URL categories. This trend is now decreasing because many end-users can recognize these types of threats. Simply put, basic attacks don't work anymore and malware authors are moving to much more stealthy attacks. The types of targeted attacks we are now seeing have both bodies and links that look very legitimate. End-users are having an especially difficult time telling the difference between the two.

Top Countries Hosting Phishing Sites over 2010



DATA DANGERS

Cybercriminals and business leaders have quickly come to realize that data is the newest form of global currency. Whether its credit cards, chemical recipes, patient records, or phone numbers, all assets have a price. Not only does the loss of assets severely damage the financial well-being of a company, it becomes a public relations nightmare when the good reputation of a company is threatened.

Here are the top 5 hosts of data stealing code in 2010:

- pc-optimizer.com
- host127-0-0-1.com
- beancountercity.com
- Otekax7c6hzuidk.com
- googlegroups.com

How big a problem is data loss?

In 2008, TJX became the poster child for data breaches when eleven men were charged with stealing over 40 million credit card numbers from the company. This affected other companies, such as OfficeMax, Boston Market, and Barnes & Noble. The sensitive information was sold to other criminal organizations in the U.S. and Europe.

On January 20, 2009, the day President Barack Obama was inaugurated, Heartland Payment Systems announced that they discovered a data breach that had happened the year before. Visa and MasterCard alerted the payment processor of suspicious activity on some of its card transactions. Data exposed through the breach included card numbers, expiration dates, and in some cases the names of customers who used debit or credit cards at Heartland's network of 250,000 businesses.

As of now, Heartland is considered the biggest data breach in history. The company set aside a total of \$140 million for related lawsuits. Heartland agreed to settle with Visa at \$60 million, MasterCard at \$41.1 million, Discover at \$5 million, and American Express at \$3.6 million. The other not so coincidental part of this case is that the mastermind behind the breach, Albert "segvec" Gonzales, was sentenced to a 20-year prison sentence in March for his involvement in the TJX breach.

Aside from the highly publicized data leakage stories presented here, it is important to note that the sheer volume of data that "drips" out of an organization is staggering. A high percentage of data loss is due to employee error, not insider theft. There are numerous cases where people simply lose their devices. Accidental loss of USB sticks, laptops, and smart phones can do catastrophic damage to the bottom line of any corporation.

In many cases, data loss is about good employees making bad mistakes. This includes sending data to themselves over the Web via personal Webmail sites (e.g., gmail, hotmail). Posting to online apps like GoogleDocs, LinkedIn, and even in the social Web. These are all ways confidential data finds its way into the wrong hands.

Whether at rest, in motion, or in use, data has become a big value item. But the cost of a data breach can be more pricey than the data itself. In addition to the strict regulations and policies that now surround data, more governments are starting to impose fines for data loss. These regulations, policies, and fines that now pertain to data vary greatly between each company, industry, and country involved.

In many cases, data loss is about
good employees making bad mistakes.

SOCIAL NETWORKING: THE BIG PICTURE, THE BIG RISKS

Social networking presents great opportunities for both forward-thinking business leaders and forward thinking criminals. Aside from the fact that social networking continues to see explosive growth, the business benefits of leveraging these sites are reaching epic proportions.

Facebook and Twitter have become an integral part of corporate campaigns and promotional activities. Forums have bridged a gap between companies and users by serving as a centralized hub of communication for both technical support and peer networking. This is especially attractive for prosumers who want to showcase their knowledge with people they haven't been able to communicate before. Any HR department or hiring manager worth their weight understands the benefits of using LinkedIn to search for qualified candidates. Public relations professionals not only use these sites for coverage, but they also have the ability to aggregate and quantify the information that fans, users, and critics post on these sites.

The bottom line is that these sites provide both financial and social benefits for all types of companies, large and small. However, many of the major social networking sites were not designed with security in mind. Think of a 99-cent application — how much security do you think goes into an application that costs 99 cents?

The unfortunate reality of the current social networking situation is that many corporations lack the knowledge and insight to make critical decisions regarding the use of these sites. More importantly, many of these decision makers don't understand the ever changing social networking threat landscape. Fear and indecision often lead to companies either granting full access to these sites or fully blocking any access to them. Both of these decisions are bad. The challenge is these sites are becoming more complicated every day. In fact, there is an increasing likelihood that social media sites will soon see the same levels of malicious content as we're currently seeing in email.

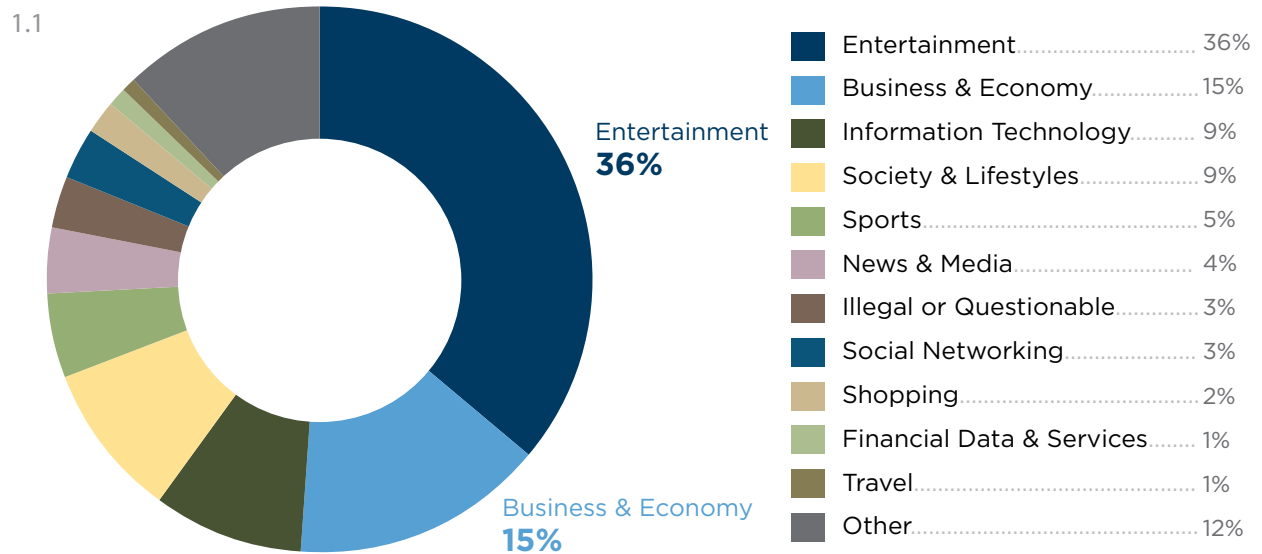
40% of all Facebook status updates have links and 10% of those links are either spam or malicious.

Business and Objectionable Content Sitting Side By Side

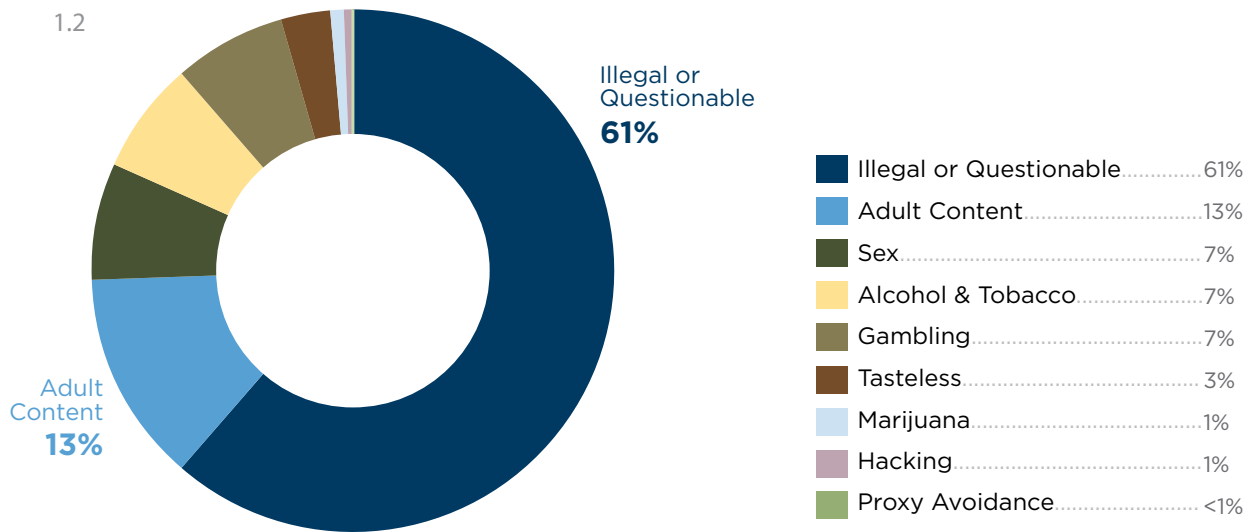
We analyzed a sample size of top 200,000 URLs in Twitter and Facebook combined to see where people were going. We compared the two sites looking at topics that fall into a general category and those that fall into categories that might be considered objectionable.

Our analysis of the continually changing content on these two websites comes from our Websense Advanced Classification Engine (ACE), which feeds into the ThreatSeeker Network.

Twitter

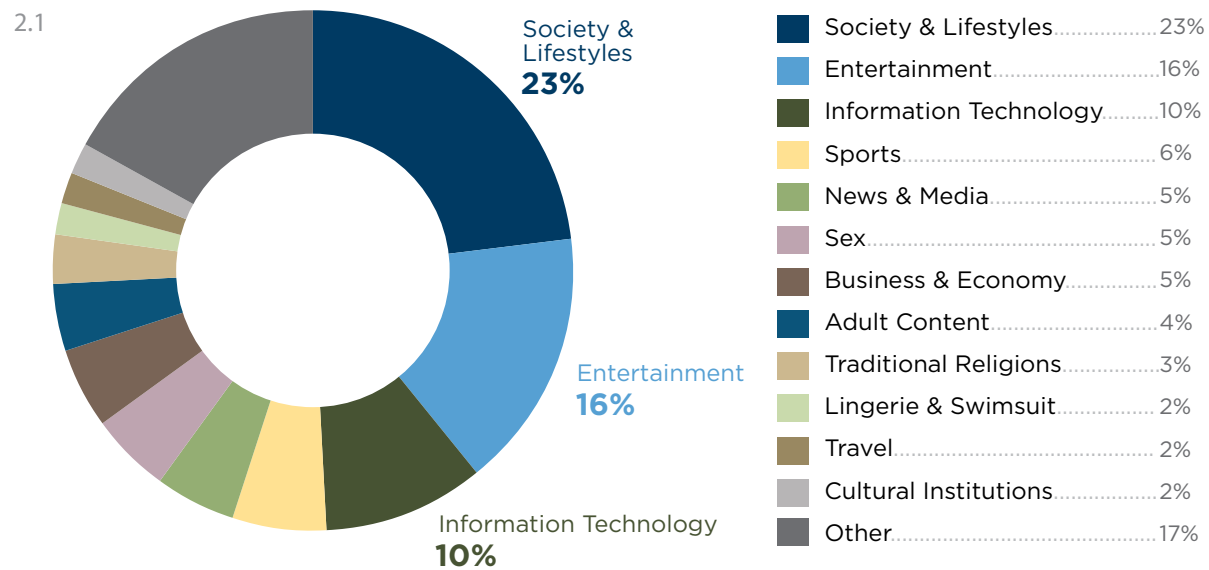


Graph 1.1 shows that among the top 10,000 popular sites, Entertainment dominated with a 36 percent majority followed by Business and Economy, Information Technology, Society and Lifestyles, Sports, News and Media.

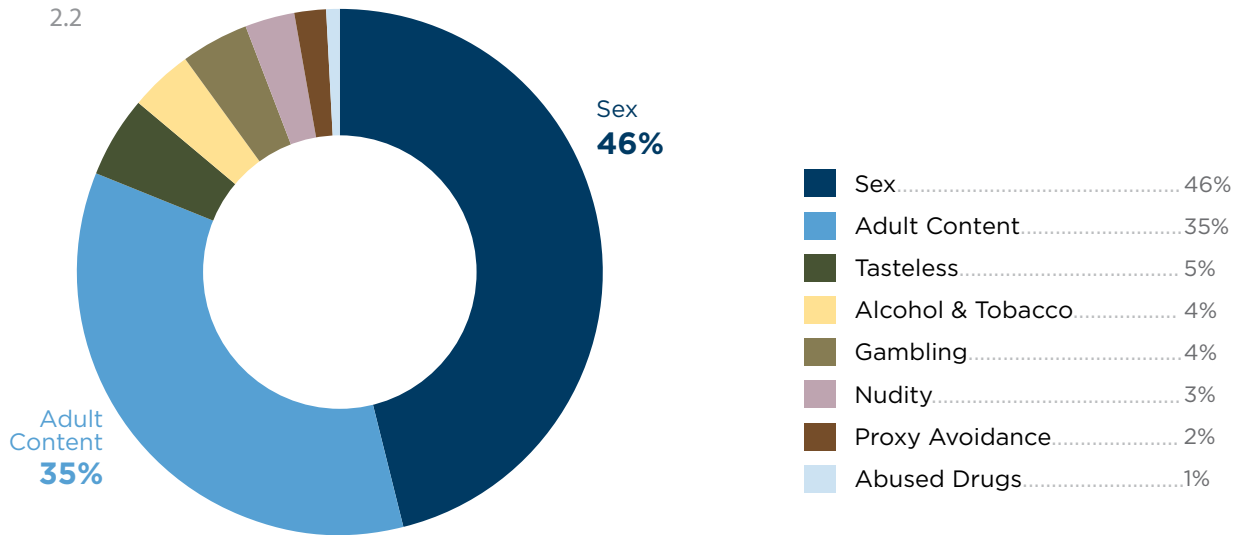


Graph 1.2 shows a breakdown of the objectionable content in the top 10,000 Twitter pages. Objectionable content made up 4.3 percent of all data. Sixty-one percent of objectionable content is Illegal or Questionable, followed by Adult Content, and Sex.

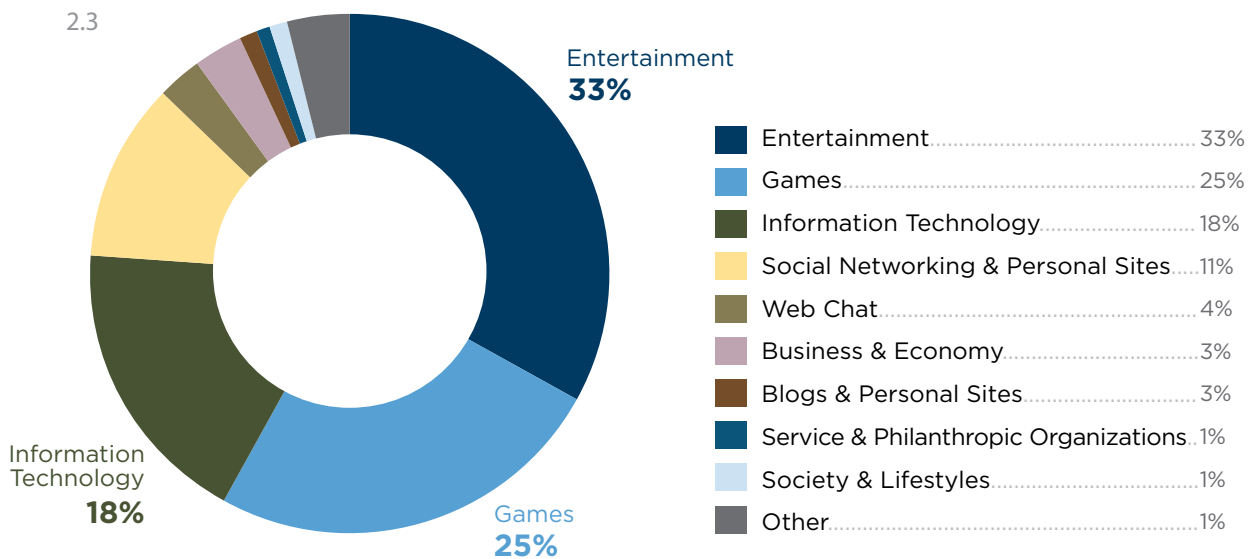
Facebook



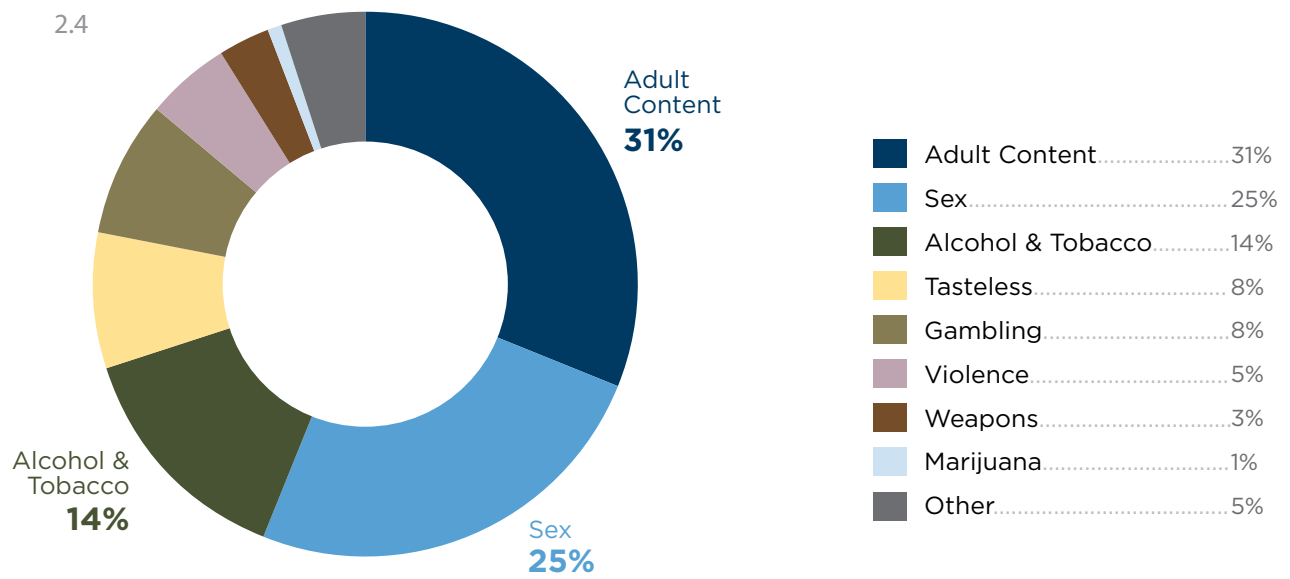
Graphs 2.1 and 2.2 represent a breakdown of the top 800 Facebook blogs by general category and objectionable category. Graph 2.1 shows that the dominating categories of these blogs are Society and Lifestyle, followed by Entertainment, and Information Technology. It is interesting to note that Entertainment is significantly lower than the Society and Lifestyle category.



Graph 2.2 shows a breakdown of objectionable categories in the top 800 Facebook blogs. Objectionable content comprises 10.47 percent of the overall data. The top three objectionable categories are Sex with 46 percent, Adult Content with 35 percent, and Tasteless with 5 percent.



Graph 2.3 shows that the dominating characteristics of Facebook applications are Entertainment, followed by Games, Information Technology, and Social Networking and Personal Sites.



Graph 2.4 shows a breakdown of objectionable categories found in Facebook applications. Objectionable content comprises 79 percent of the overall data.

WEBSense SECURITY LABS: MAJOR 2010 DISCOVERIES

Office.Microsoft.Com Search Results Can Lead to Rogue Antivirus

Attack Date: 01/08/2010

Attack Details: Websense Security Labs and the Websense ThreatSeeker Network detected that search results on office.microsoft.com can lead users to a Rogue AV page. Users looking for information related to help with Office products on Microsoft's own site are being targeted. Users may be unaware that when they type in search queries on the site, Microsoft scours its own website for results but also pulls in results from the broader Web. Since the URL for the search results begins with http://office.microsoft.com, this is particularly troubling for users who trust sites simply because of their reputation. The malicious URL served as a redirect to a very real-looking virus scan and warning page presented by a Rogue AV. At the time of discovery, the executable used in the exploit was only recognized by one of the 41 AV engines on Virus Total.

Black Hat SEO Caused Malicious Search Results for Haiti Earthquake

Attack Date: 01/13/2010

Attack Details: Websense Security Labs and the Websense ThreatSeeker Network discovered that searches on terms related to the earthquake in Haiti returned results leading to a rogue antivirus program. The earthquake, which happened on Tuesday January 12, near Port-au-Prince, had a magnitude of 7.0 and is said to be the most powerful earthquake ever to hit Haiti. People around the world had searched the Internet to find the latest updates on the disaster. People were looking to make charitable donations, trying to discover the extent of the calamity through photos or videos, and looking to see what their favorite artists and musicians were saying about the disaster. Unfortunately, the bad guys use major crises and events like this to spread their malicious code. The malicious code had less than a 20 percent detection rate by the major antivirus vendors, according to Virus Total.

Oklahoma Tax Commission Site Compromised

Attack Date: 01/29/2010

Attack Details: Websense Security Labs and the Websense ThreatSeeker Network discovered that the home page of the Oklahoma Tax Commission website had been compromised with malicious script code. After the page was loaded, the browser executed the injected script in the background. The injected script code would go through a series of deobfuscation techniques that ultimately took the victim computer to an attack website without the victim's consent or knowledge.

Malicious Spam Campaign Spoofs Google Job Application Response

Attack Date: 02/1/2010

Attack Details: Websense Security Labs and the Websense ThreatSeeker Network discovered a new malicious spam campaign that spoofed Google job application responses. The messages looked very well written and were so believable that there were probably excerpts from actual Google job application responses. Typically, spam has grammatical errors or spelling mistakes that make the messages obviously unofficial and act as red flags. The text of these messages, however, had no such mistakes, making them much more believable, especially if the target really has applied for a job with Google. The From: address was even spoofed to fool victims into believing the message was sent by Google. The messages had an attached file called CV-20100120-112.zip that contained a malicious payload. This is where the message got suspicious, because the contents of the .zip file had a double extension ending with .exe. The attackers attempt to hide the .exe extension by preceding it with .html or .pdf, followed by a number of spaces and then the .exe extension.

Speed Testing Site Chinaz.com Compromised

Attack Date: 05/25/2010

Attack Details: Websense Security Labs and the Websense ThreatSeeker Network discovered that the speed testing site, chinaz.com, had been compromised. Chinaz.com is a very famous Web master site that provides technical and resource downloading services in China. The daily traffic to this site is over 50,000 hits, and it has a very high Alexa rank of 179. The injected subdomain, speed.chinaz.com, is the page that supplies tools for testing the speed of websites. This site first redirects to a JavaScript file in its own path. The malicious code injected by the cyber criminals had a payload that contained two parts (ap.js, and the obfuscation code in the script tag). After analyzing this, we noticed that it was used to target the IE vulnerability (MS10-018), which downloads an executable file named dn.exe. This had a good detection rate by most AV vendors, however dn.exe would download and execute remote files and send local information to a remote server. The process had disguised itself as an AV component, while at the same time suspending the AV software.

Game Channel of MOP BBS Compromised

Attack Date: 05/30/2010

Attack Details: Websense Security Labs and the Websense ThreatSeeker Network discovered that the game channel of MOP BBS had been compromised. Mop.com is one of the largest and most influential forums in China. It was the birthplace of Chinese network culture and has grown into a website with integrated forums, news, games, and entertainment to become a huge multimedia information platform. Mop.com has over 50 million registered users and over 200 million daily views making it the world's 275th most popular website according to Alexa. The website is especially popular among World of Warcraft fans. This site contains a reference to the JavaScript file ajax.js which was modified and injected with malicious code by cyber-criminals. The compromise used a technique often used by Black Hat SEO attackers in which only the visitors who open the page from baidu.com search results, the very popular search engine in China, will get the malicious code. The code then does another check to see if the popular Chinese antivirus software 360 Safeguard is installed. If not installed, the code would continue to exploit the PC (step 2 in the chain). After that, it will go on to redirect to the two URLs. Both sites have the same payload and both utilize the Microsoft Internet Explorer vulnerability MS10-018 to infect the user. After a quick analysis, we found that the shellcode in the exploit would download the executable remote file called 55.exe. The file is encrypted and has very low antivirus detection. The shellcode in the exploit is then used to decode the file. After being decrypted, the file is detected as an online game information stealer.

World Cup Targeted by Malicious Spam Campaign

Attack Date: 06/11/2010

Attack Details: Websense Security Labs and the Websense ThreatSeeker Network detected a new wave of interesting malicious emails. At the dawn of the eagerly anticipated World Cup tournament we expected to be inundated with suitably themed spam. The sample we encountered was a little different from the usual sample, because the technique used may not raise suspicion. We saw over 80,000 email messages in this new campaign, which used an HTML attachment with an embedded JavaScript. Upon execution, this script led to a malicious website.

Songlyrics.com Compromised

Attack Date: 09/16/2010

Attack Details: Websense Security Labs and the Websense ThreatSeeker Network detected that the popular site Songlyrics.com (with approximately 200,000 daily page views and 2,000,000 unique visitors) was compromised and injected with obfuscated malicious code. When a user would access the main page of the song lyrics site, injected code redirected to an exploit site loaded with the Crimepack exploit kit. Attempted exploits resulted in a malicious binary (VT 39.5 percent) file that would run on the victim's computer. Once infected, the machine became another zombie-bot in the wild. It is interesting to note that the malicious code injected on Songlyrics.com used a similar obfuscation algorithm as Crimepack, a prepackaged commercial software used by attackers to deliver malicious Web-based code. At the time of discovery, the majority of pages served by Songlyrics.com were compromised.



Crimepack has become one of the best-selling exploit packs on the market due to its huge number of pre-compiled exploits offering a great base for the “drive-by-download and execute” business.

THE NEXT 12 MONTHS

Here are some emerging trends and predictions by Websense Security Labs researchers:

Smartphones: Some mobile platforms including the iPhone have already been attacked. The continued consumerization of these phones and the increasing amounts of financial data that touch these devices make them ripe future targets. Also, there is a sizeable variance between the quality of available mobile applications. These applications will open the door for unintended security vulnerabilities. Jailbreaking iPhones is just a preview of the dark alley that many of these phones will enter. Legitimate apps will easily be repurposed for spam and phishing attacks.

Hate and Terrorism: Photographic evidence of terrorists hiding in caves doesn't serve as good examples of the level of sophistication in which these groups operate. We've already seen a rise in the presence of these organizations on the Web. Numerous groups will continue to focus on the Web to recruit members, make money, and commit various crimes. We also expect a tightening of the organizational structures in which these groups operate.

Blended Attacks: SEO optimization combined with rogue AV and email containing data stealing components will not slow down in the coming 12 months. Relying on reactive security measures such as standalone AV will simply fail to provide adequate protection against these sophisticated techniques that combine Web, data loss prevention (DLP), and email.

Spam and Email: Spam campaigns will continue to target the walls of Facebook and other social networking sites. Email attacks will continue to become more sophisticated with a focus on links and attachments to help disguise their bad intentions.

Botnets: As in the past, the majority of attacks will rely on botnets. These are very cost-effective for cybercriminals and they have enough range to reach far and wide.

Old Vulnerabilities: Adobe Reader and Microsoft Internet Explorer were prime targets throughout 2010, and there is no sign of a change in course on the part of the hackers. Old vulnerabilities will be subject to no shortage of exploits in the coming year.

DLP and the Dynamic Web: The top 100 websites feature constantly changing content with billions of varied page visits per site. Many companies will find themselves caught off guard, placing their data at risk, due to bad business practices regarding the sensitivity of data on these sites.

SUMMARY

“Education is critical. People need to know what they should be defending against.”

Jay Liew, Websense Security Researcher

The evolution of the threat landscape during 2010 has revealed new security threats and confirmed the ongoing menace of well-known threats.

Our research underscores how running stand-alone antivirus products against today's content-focused threats is ineffective, as are threat signatures and URL filtering. Our research also shows that a data loss prevention solution is no longer a “nice to have” option but should be considered a core requirement. The Web has transformed into a business and application platform. Real-time social networking sites will continue to dominate the landscape. Hackers will continue to mix social engineering tricks with modern blended threats making the Web more complicated than ever before.

The blended nature of today's threats means that all security measures must integrate email, Web, and data technologies. 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.

Stay informed with 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 websense.com, Websense Security Labs Alerts are now available through email.

Sign up to have the latest security warnings on malicious Internet events, including spyware, phishing and corrupted websites, sent directly to your inbox as they are discovered by Websense Security Labs.

Written by Jon Crotty.

About Websense

Websense, Inc. (NASDAQ: WBSN) is the leading provider of unified content security. We are the global leader in unified Web, data, and email content security solutions, and provide the best security for modern threats at the lowest total cost of ownership to tens of thousands of enterprise, mid-market, and small organizations around the world. Distributed through a global network of channel partners and delivered as software, appliances, and Security-as-a-Service (SaaS), Websense content security solutions help organizations leverage new communication technologies and enable collaboration and the productive use of Web 2.0 business tools. We do this while protecting organizations from advanced persistent threats, preventing the loss of confidential information, and enforcing Internet use and security policies. Websense is headquartered in San Diego, Calif., and has offices around the world.

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>