WEBSENSE® Security Labs™

First Half 2006

Security Trends Report

Websense Security Labs
Research Team

Websense Security Labs researches today's advanced internet threats, focusing on malicious websites, phishing, and other emerging threats associated with spyware, keylogging, and instant messaging and peer-to-peer use. This report summarizes findings for the first half of 2006 and presents projections for the upcoming period.

Contents

Introduction

This report summarizes significant findings during the first six months of 2006. This report also evaluates these threats in terms of trends and, where possible, includes projections for the coming period and beyond.

> *Unless otherwise noted, all information is from Websense Security Labs and its research.*

The first half of 2006 in brief

High-tech crime goes commercial…

In the first half of 2006, we have seen malicious code become more covert, less recognizable, and more targeted toward financial gain. Not only has the code itself become more sophisticated, but the infrastructure supporting its creation and spread has also become more complex. Cyber-criminals are now more creative, organized, and business savvy. True "companies" have emerged, producing and selling toolkits and developing business partner programs that enable less-technical, "traditional" criminals to use the web to steal data and make money – lots of it.

> *Of the sites designed to steal credentials, almost 15% are derived from toolkits.*

Client and server exploits continue…

Over the last six months, we have seen increased exploitation of both web servers and web browser/client technologies. Automated vulnerability scanning for server and client exploits is becoming more intelligent, and attackers are taking full advantage.

Phishing	
Phishing emails	↑
Phishing keyloggers	↑
Phishing redirectors	↑
Pharming	→
Malicious Websites	
Social engineering / deception techniques	↑
Keyloggers	↑
Toxic blogs, personal storage, and social networks	↑
Malicious Code	
Spyware – keyloggers	↑
Spyware – industrial espionage	↑
Cyber-extortion	↑
BOTs	→
Hacking Websites and Hacking Tools	
Hacking sites and tools	↑
P2P, IM, Chat	
Bots – using P2P, IM, chat	→
IM – using vulnerabilities or social engineering and a malicious website	↑
P2P – spreading malicious code	→
P2P botnets – using P2P to control	↑

> *In H2, 2006 35% of all malicious websites are hosted on web servers that have been compromised.*

Drop in benign, increase in malevolent…

Websense Security Labs has seen a 100 percent increase in sites designed to install keyloggers, screen scrapers, and other forms of crimeware. Conversely, the organization has seen more than a 60 percent drop in websites designed merely to change user preferences, such as browser settings.

More botnets using P2P, IM, and chat…

In H1 2006, we noted more botnets using P2P technologies to gain control, making it more difficult to disable them. The use of the web to control botnets has also increased, allowing botnet owners to more easily control the machines via a web page.

Ability to categorize applications within search engines…

Previously, mining search engines was the primary method used to identify websites hosting active content exploit code. During the first half of 2006, Google began categorizing applications within its search engine. Researchers from Websense Security Labs use this new technology to help find viruses and malicious code hosted on websites by searching on different patterns within the code, such as known packer routines and Microsoft Windows calls that are known to be used for nefarious purposes.

Increases in phishing targets…

During H1 2006, we saw a significant increase in the number of phishing targets. In fact, Websense Security Labs sees as many as 8–10 new targets every day (with an average of 3–6 daily). We also note that phishing toolkits are now being used to enable easy phishing. For example, one site may offer as many as 50 different banks, with separate directories for each one that contain individual attack dynamics. For example:

/wellsfargo/

/Citibank/

/creditunion/

More extortion, with better encryption…

We saw more cases of – and more sophisticated use of – cyber-extortion during H1 2006. Along with the higher numbers, we note better encryption, making it harder to recover the data and reverse engineer and develop effective countermeasures.

As we predicted…

Many predictions made in previous reports came true during the first half of 2006.

- The number of phishing incidents continued to rise. On average, Websense Security Labs sees 3–6 new targets every day.
- Web-borne worms and blogs continued to be avenues for exploitation.
- Voice-Over-Internet-Protocol (VOIP) phishing began to occur.
- Blogs, personal web hosting, and social networking sites continued to be utilized to host exploits, phishing, and fraud.
- Cyber-criminals continued to use innovative social engineering techniques to further their exploits.

Phishing, Malicious Code, and Crimeware

Lines between phishing, malicious code, and crimeware continue to blur

During H1 2006, we observed increased use and availability of toolkits that enable easy phishing. We have also seen more cases of malicious code injecting itself into a web browser.

Phishing

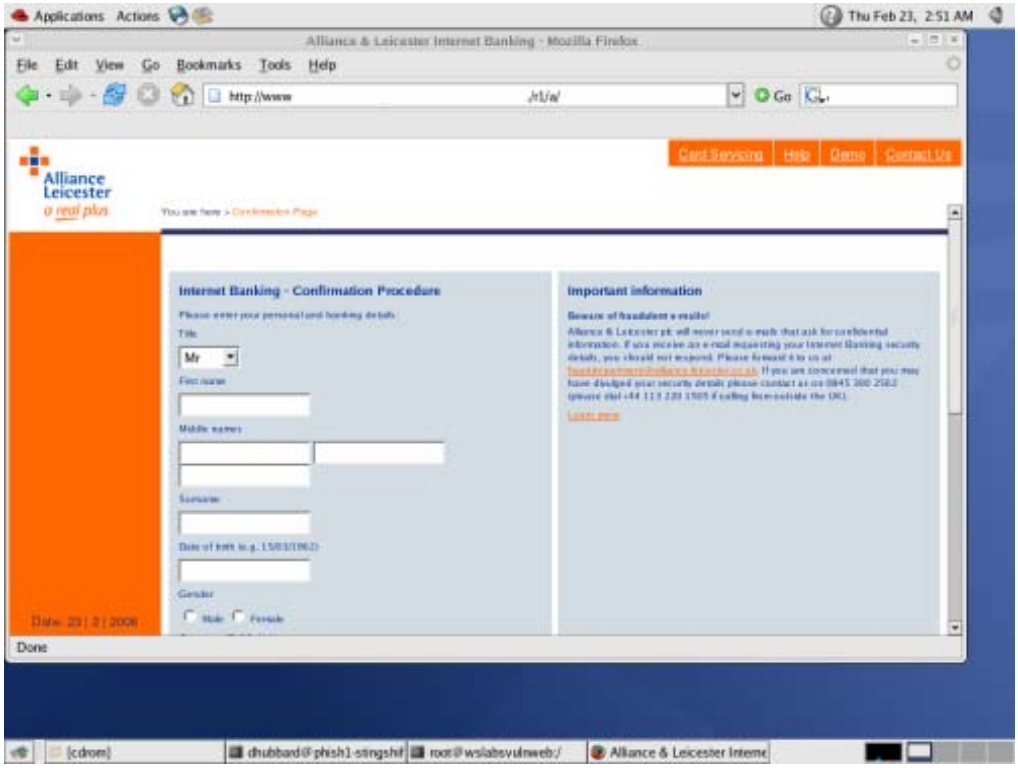
Significant rise in the number of phishing targets

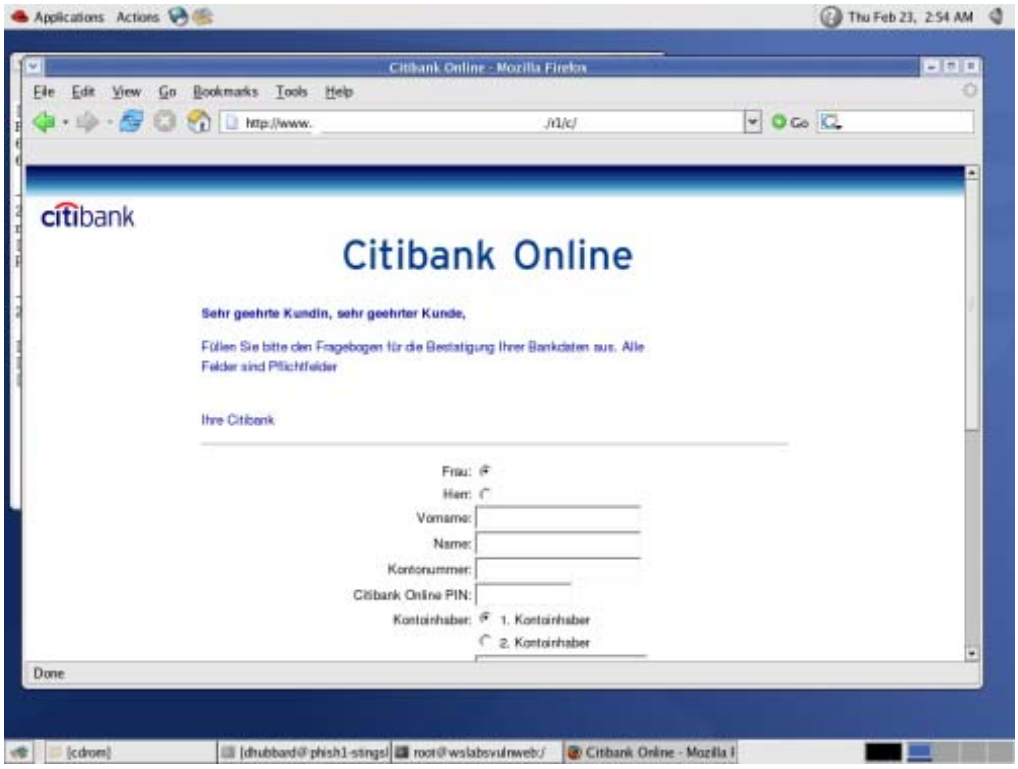
In H1 2006, we saw a significant increase in the number of targets. During this period, Websense Security Labs logged an average of 3–6 new targets every single day.

Toolkits also continued to be used to enable phishing. During this period, we reported a significant increase in the number of phishing kits used to host multiple target brands on a single host and deploy similar attack code on several machines. One such example is the "Rock Phish Kit." This kit appears to have surfaced around November of 2005, but the frequency of its use is growing. Following are some characteristics of sites created using this kit.

- Sites often use either an IP address or a fraudulent domain name.
- Sites usually have /rock/ or /r/ in the URL path, followed by an alpha character.
- Quite often the letter after the /r/ matches the target name (e.g., www.samplerockphish.com/r/b = barclays).
- Sites are usually hosted in Asia.
- Sites use the same PHP script to post the data.
- Sites often use JavaScript tricks to replace the browser toolbar and disable keyboard functions such as Cut and Paste.

One site created using the Rock Phish Kit hosted multiple phishes with six different brand names. This site targeted Alliance Leicester, Citibank, Deutsche Bank, eBay, and Hallifax. A couple examples of the phishes appear below.





Phishing reports in H1 2006

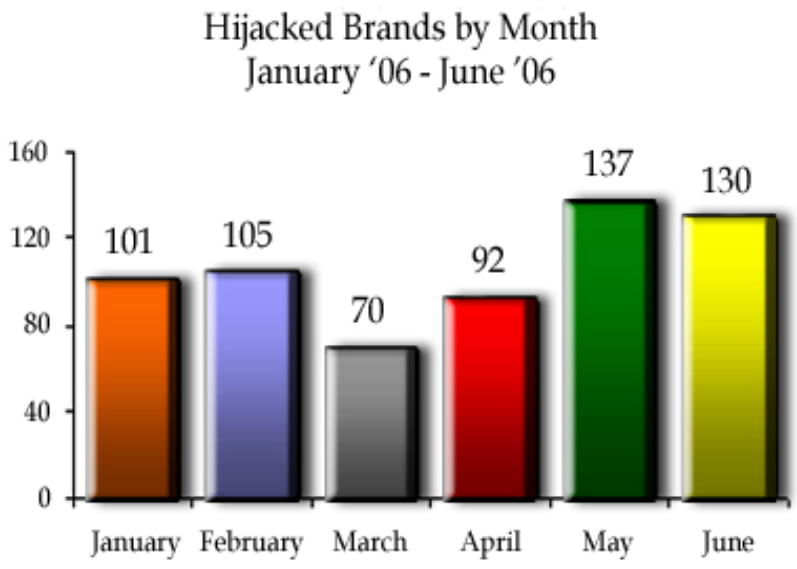
The illustration that follows shows the increase in the number of phishing reports received from January through June 2006. Note the sharp increase from May to June 2006.

Courtesy Anti-Phishing Working Group

Targeted brands

The illustration that follows shows a drop in the number of hijacked brands in March, with that number nearly doubling by May 2006.

> *Any brand that does commerce on the internet should be aware of the potential for customers to be targeted.*



Courtesy Anti-Phishing Working Group

Changes in types of phishes

We have seen a marked increase in the number of instances of malicious code that injects itself into the web browser in order to steal information by grabbing form inputs. This is a direct result of a kit called “Nuclear Grabber” that is for sale on the internet. (See the “Hacking Websites and Hacking Tools” section for more information.)

Throughout December 2005, we reported a number of cases where browser and operating system vulnerabilities were being used to install potentially unwanted software onto end-users’ machines without user intervention. In several cases, dozens of pieces of code were installed, often reporting false information in order to entice end users to remove spyware from their machines.

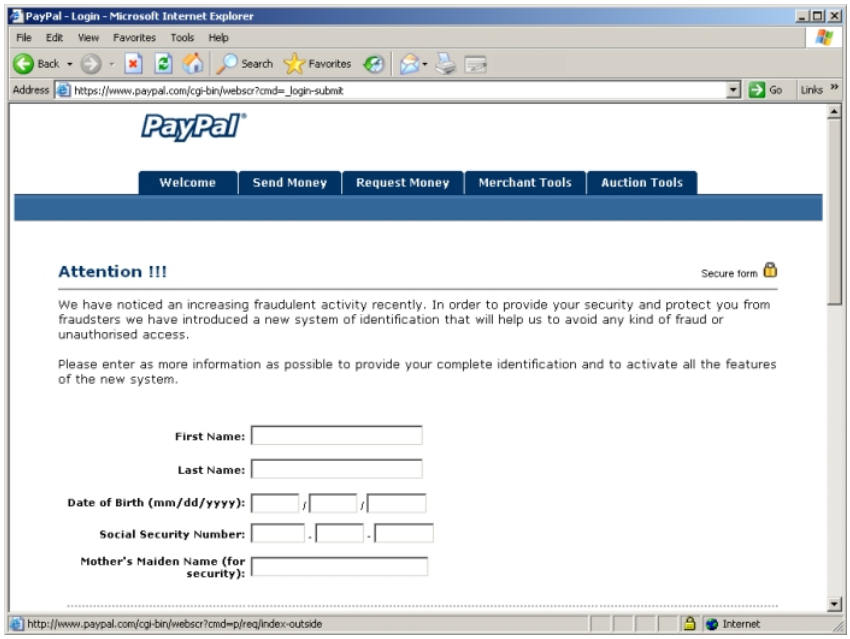
We are now seeing some of those same entities using their exploit code to install more reprehensible crimeware, such as keyloggers and phishing traffic redirectors. This code is designed to steal information, as well as install potentially unwanted software.

One keylogger (see example below) monitors for every POST request made by the client computer (such as a logon to a banking website) and sends the captured information to a URL running a script named ”x25.php.” This program also injects itself into the Internet Explorer process and silently redirects attempts to log in to specific financial sites.

The malicious code has additional functionality. When visitors to one of a set of predefined websites attempt to log in, they are redirected to a fraudulent site, which asks for additional credential information.

```
POST /gamma/x25.php?
Content-Type: multipart/form-data; boundary=swefasvqdvwxff
....Host:
Content-Length: 457
Connection: Close
User-Agent: Mozilla/4.0
Host:
Cache-Control: no-cache

...--swefasvqdvwxff
Content-Disposition: form-data; name=datafile; filename="data.str"
...Content-Type: application/octet-stream

...4.C!...Application: c:\program files\internet explorer\iexplore.exe
REQUEST:
HEADERS:
POST /cgi-bin/webscr?cmd=_login-submit HTTP/1.1
Host:
Referer: http://www.paypal.com/

POST_FORM:
login_email=user@domain.com<-- Captured Login
login_password=mypassword<-- Captured Password
submit.x=Log+In
form_charset=UTF-8

.
--swefasvqdvwxff--
```

The circled area shows where the user’s password is stolen.



In this screen, we connected to PayPal.com. After entering any user name and password, we were redirected to a fraudulent page where personal information was requested. The toolbar still shows the original site; however, the site that is hosting this code is on another server not owned by PayPal.

Keyloggers and screen scrapers

We have also seen increases in screen-scraping malicious code. This code allows criminals to take screenshots of an end user's desktop, in order to collect information such as usernames and passwords. They use screen-capturing technology because, in some cases, ecommerce and financial sites feature virtual keypads that use a mouse for inputting credentials and for authenticating users instead of a keyboard.

Spear phishing

During H1 2006, employees and customers of a number of companies and service providers were targeted directly with spear phishing attacks. In these attacks, lists of ISPs, commerce, and banking site customers have been targeted specifically, as opposed to "casting wide nets."

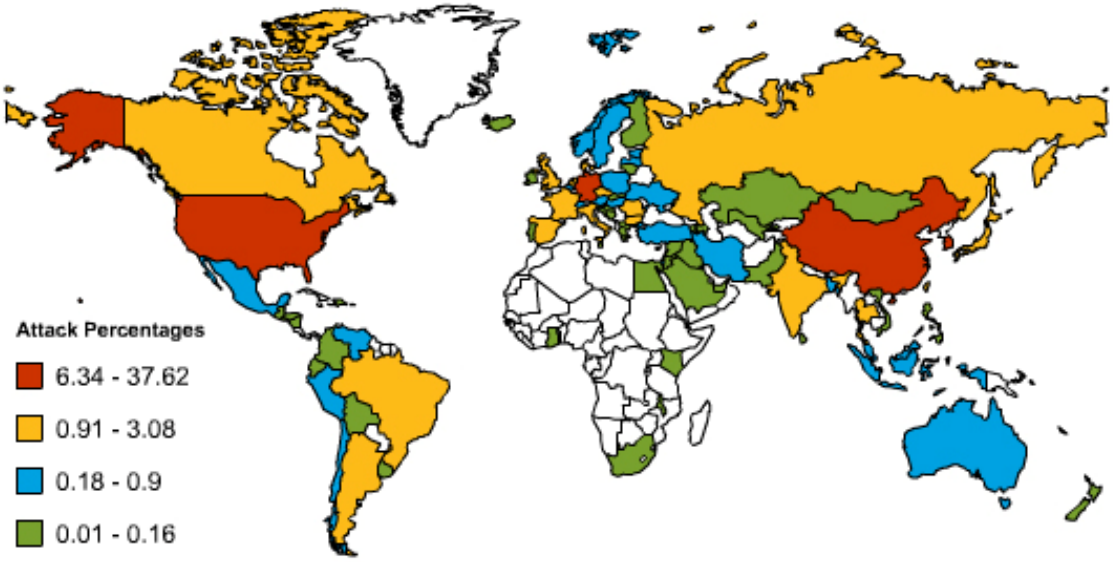
Redirectors

Redirectors transfer end-user network traffic to a location other than that intended by the user. The redirector category includes crimeware that changes host files and other DNS-specific information, browser-helper-objects (BHOs) that redirect HTTP traffic to fraudulent sites, and crimeware that may install network-level drivers or filters to redirect to fraudulent locations.

In the first half of 2006, we observed that BHOs were used increasingly as a means to redirect preselected traffic without a user's knowledge.

Increases in international phishing and crimeware

Websense Security Labs continued to provide statistics for the monthly Anti-Phishing Working Group (APWG) reports tracking the geographical location of hosting for phishing sites. Late in the first half of 2006, we saw the United States for the first time ever dip below 30% of the total percentage of sites. China and Korea continue to be the second and third most popular location for hosting phishing attacks.



Phishing site locations

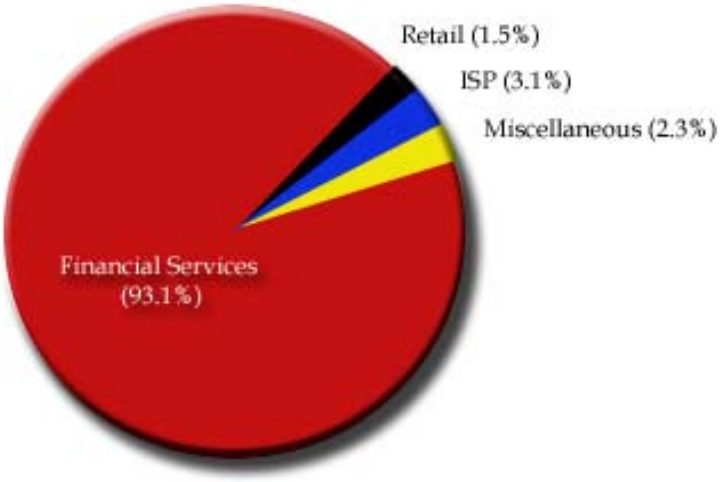
Reasons for changes

On the anti-fraud front, countermeasures continue to improve. In addition, the noncommercial, volunteer-driven, Phishing Incident Reporting and Termination (PIRT— http://wiki.castlecops.com/PIRT) squad was formed. This organization does a good job of taking sites down once reported.

Unfortunately, the criminals and their methods are evolving very rapidly, adapting quickly to developed countermeasures. They are using technologies such as “fast flux” DNS to change their name servers and site locations very quickly in order to prevent shutdown. Additionally, proxy servers, redundancy, and fail-over on the server side are all new, emerging techniques.

H1 2006 phishing statistics

Although the financial industry continues to be plagued by phishing (see illustration that follows), we are seeing increases in the number of non-financial organizations being targeted. Myspace, Google, and Yahoo are the top three web entities being targeted. Not only are these sites targets for phishing, but they are also being targeted as locations for hosting and distributing malicious code, adware, and as open redirectors.



Courtesy Anti-Phishing Working Group

Malicious Code

More covert, more aimed at profit

During H1 2006, we saw that code is becoming more covert, less recognizable, and more targeted at profit. We also noted that the underground environment for malicious code – its infrastructure of entities, individuals, and groups – has also become more sophisticated. Code developers are becoming more creative, better organized, and more business savvy. Companies have emerged that market tools and kits which are sold or traded online. These toolkits enable less-technical criminals to capitalize on this burgeoning market, without requiring them to even learn the technology.

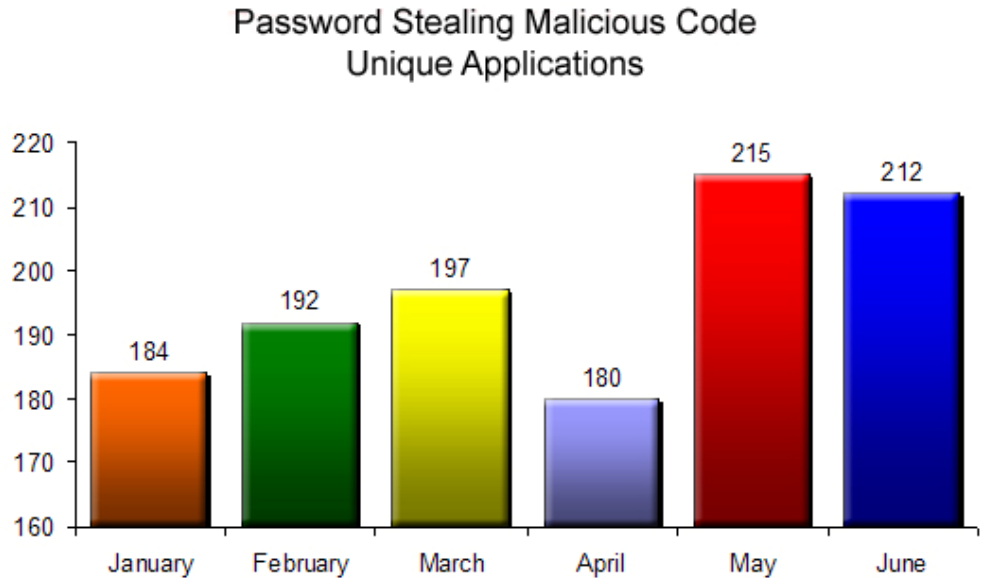
Crimeware / Spyware

Banking Trojans

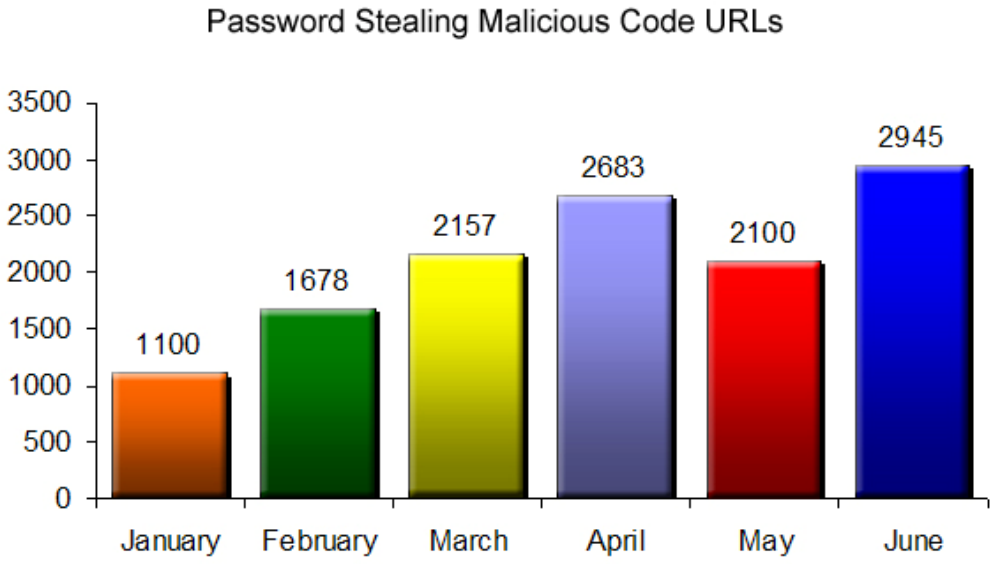
Unlike most generic keyloggers, phishing-based keyloggers have tracking components which attempt to monitor specific actions (and specific organizations, most importantly financial institutions and online retailers and ecommerce merchants) in order to target specific information, such as access to financial-based websites, ecommerce sites, and web-based mail sites.

Phishing-based Trojans in H1 2006

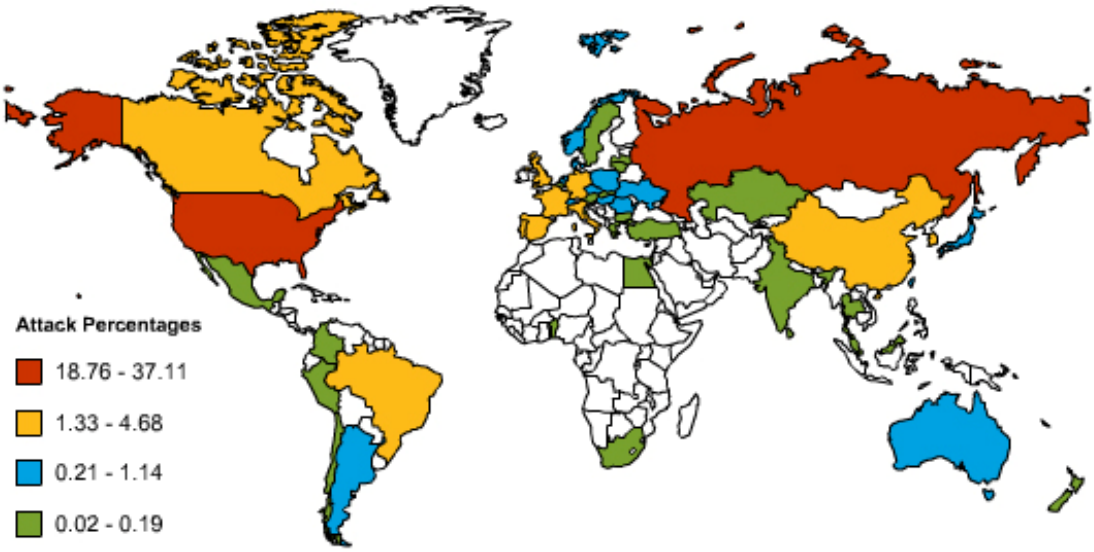
The illustration that follows summarizes the distribution of phishing-based Trojans (keyloggers with unique variants) during H1 2006.



The illustration below shows a dramatic increase in the number of websites hosting keyloggers – from 1,100 to 2,945 – during the first half of 2006.



The illustration that follows shows the locations that host crimeware code. As the figure shows, Russia and Brazil are the second and third most used nations to host crimeware code.



Crimeware site locations

Bots

In H1 2006, we saw several reports of a new worm, "Nugache," which spread on AOL/MSN Instant Messenger networks and as an email attachment by exploiting several workstation vulnerabilities. The worm opens a back door on TCP port 8, and installs a bot to wait for commands from the attacker. The command and control channel that is used is unique, as the bot appears to connect to infected peers instead of a static list. A peer-to-peer Command and Control channel makes it more difficult to block commands issued to the bot. The traffic over this channel also uses obfuscation in an attempt to bypass intrusion detection systems.

> *A bot is a software program that interacts with other network services intended for people as if it were a person. One typical use of bots is to gather information. The term is derived from the word "robot." The most common bots are those that covertly install themselves on people's computers for malicious purposes, and that have been described as remote attack tools.*

We are also seeing increasing use of shellbots – bots that run on non-Windows operating systems, such as Linux and Solaris. These servers are quite often used because they are often more reliable than end users' PCs that have been infected on broadband, they stay up longer, and they may also have more bandwidth from which to send SPAM and launch attacks.

Cyber extortion

During this period, we noted improvements in encryption, as well as several new variants.

Malicious Websites

Huge increase in number of sites designed to steal

In H1 2006 we saw a 100% increase in the number of sites designed to install keyloggers, Trojan droppers, and hosting for compromised information.

Malicious code toolkit profiteering

Of the sites designed to steal information, 15% are derived from toolkits. These toolkits range in price from $30 to $3,000, and even feature user manuals to help neophyte cyber-criminals get their “businesses” up and running quickly. They also advertise their ability to defeat antivirus (AV) technologies and often publish their testing statistics against the latest signature engines to prove their craftiness.

The illustration below shows the results of testing the latest toolkit (WebAttacker) against the latest AV signatures from specific companies. The screen shot demonstrates how the toolkit makers are testing against the latest signature databases that are not classifying their code.

Эксплойт - Web-Attacker IE0604 не обнаруживается следующими антивирусами:

Названия Антивируса	[Версия]	[Дата баз]
Doctor Web	4.33	-
NOD32 Antivirus	2.5	-
McAfee VirusScan	10.0.27	-
Norton Antivirus	2006	13.04.2006
Kaspersky Antivirus	5.0.391	14.04.2006
Panda Titanium Antivirus	2005	11.04.2006

Drop in number of sites with no malicious intent

We noted more than a 60% decrease in the number of sites designed to change preferences, such as browser settings, with no malicious intent. These sites do not log keystrokes or steal credentials.

Browser and operating system vulnerabilities

At the end of 2005, Websense Security Labs was credited with the discovery of the WMF zero-day exploit. In H1 2006, we saw a continued trend of browser exploits.

The “IE CreateText” zero-day exploit was released in March 2006. Immediately, websites started coming online that used exploit code to install and run malicious software without user interaction.

During the first half of 2006, we started using an automated means of discovering vulnerabilities within browsers and operating systems. Technologies such as “fuzzers” are also increasingly being used.

A fuzzer is a tool used by security professionals to test a specific parameter of an application. Typical fuzzers test an application for buffer overflows, format string vulnerabilities, and error handling. Other, more advanced fuzzers test for directory traversal attacks, command execution vulnerabilities, SQL Injection, and other vulnerabilities.

As we reported in our IE CreateText alert, in this exploit, email messages contain excerpts from actual BBC news stories and offer a link to "Read More." Users who follow this link are taken to a website that is a spoofed copy of the BBC news story from the email. This website exploits the unpatched createTextRange vulnerability and is used to download and install a keylogger. This keylogger monitors activity on various financial websites and uploads captured information back to the attacker.

Users who follow a “Read More” link are taken to a website that is a spoofed copy of the BBC news story from the email.

Microsoft reacted to notification of this threat by issuing a “critical” security bulletin.

Toxic blogs

As the use of blogs, personal storage sites, and social networking websites continues to increase, we are witnessing increased use of them for malicious purposes. In June 2006, several Myspace pages were infected with code that was designed to install adware onto users' machines through browser exploit code within an IFRAME.

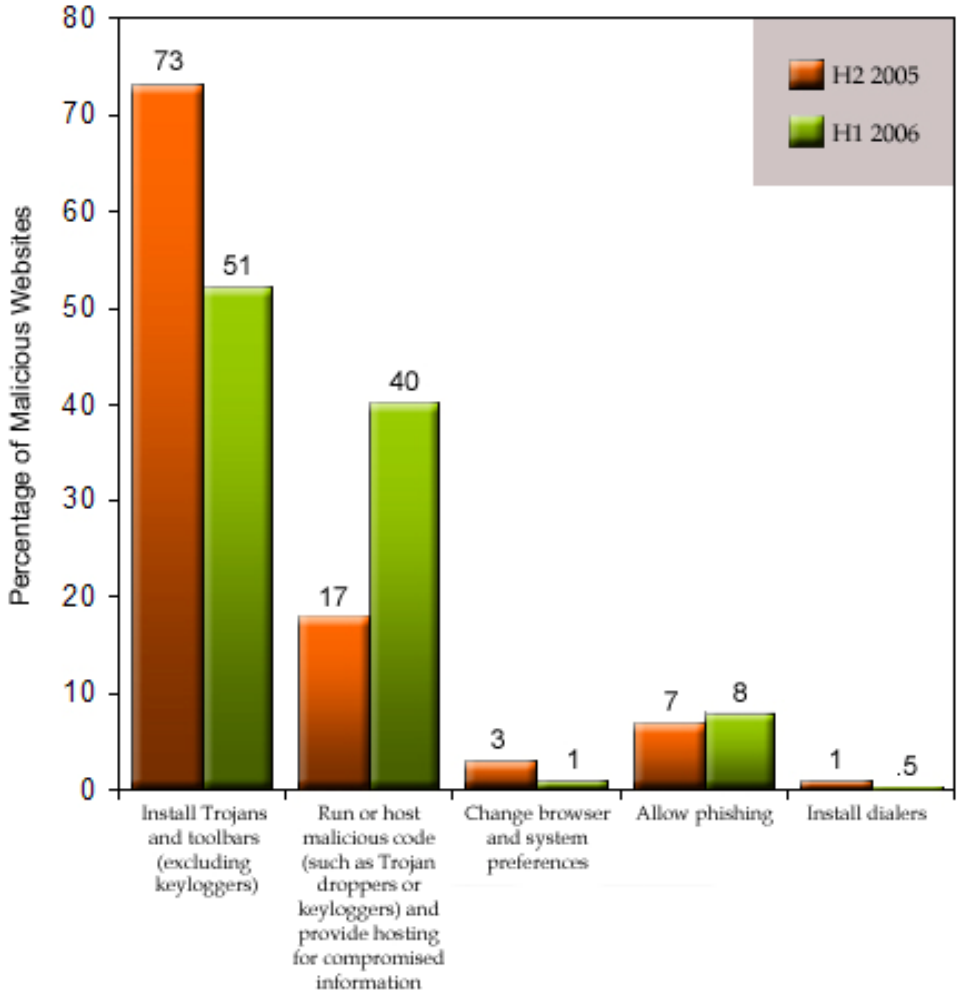
In July 2006, Yahoo! fell victim to a browser exploit that used Yahoo! mail to spread to all contacts within a website address book. Yahoo! mail incorrectly filters the "onload" attribute out of <img> tags in HTML emails. The "onload" script is executed upon receipt of the malicious email. The script utilizes the Yahoo! QuickBuilder tool to mine all the email addresses from the victim's inbox. The worm then mails a copy of itself to each of these addresses and sends the list of addresses to a third-party site where the addresses can be used by the attacker for other purposes. Finally, the worm redirects the victim's browser to a third-party site that displays numerous advertisements and could potentially deliver additional malicious code.

At the time the Websense Security Labs alert was sent, messages sent by the worm used "av3@yahoo.com" as the From address and "New Graphic Site" as the Subject. However, these values are easily changed by the attacker.

The exploit succeeds even if users' preferences are set to block images in HTML emails.

Increase in malicious websites during H1 2006

The illustration that follows identifies the changes in malicious websites from H2 2005 to H1 2006.



Hacking Websites and Hacking Tools

Exploit code toolkits for profit

Toolkits

During H1 2006, we saw a dramatic increase in the number of toolkits created. These toolkits help would-be cyber-criminals get their new web-based businesses up and running very quickly. How-to manuals are even available for sale. These toolkits range in price from $30 to $3,000.

Of the sites designed to steal credentials, 15% are derived from toolkits and a stunning 40% are hosted on machines which have been compromised. This is clear evidence of the new “professionalism” of the attackers. The increases are not solely the result of increases in the numbers of entities set up to assist “non-technical” users by selling exploit kits, but also the use of network-level vulnerability exploit tools that allow attackers to infect sites to host their code.

The increasing number of compromised web servers is also a result of the large numbers of web server technology vulnerabilities in scripting languages, bulletin board software, and other web-based technologies.

How much would an attacker be willing to pay for exploit code? As the illustration below shows, 38.2% of visitors to a specific website said they would be willing to pay between $100 and $300. Another 14% said they would be willing to pay more than $1,000.

WebAttacker

The WebAttacker toolkit, available on a Russian website, enables even the most neophyte computer users to easily install exploit code on their websites. When a user visits an infected site, a Trojan horse is downloaded and run. It can log keystrokes, download additional code, or open backdoors on the user's machine.

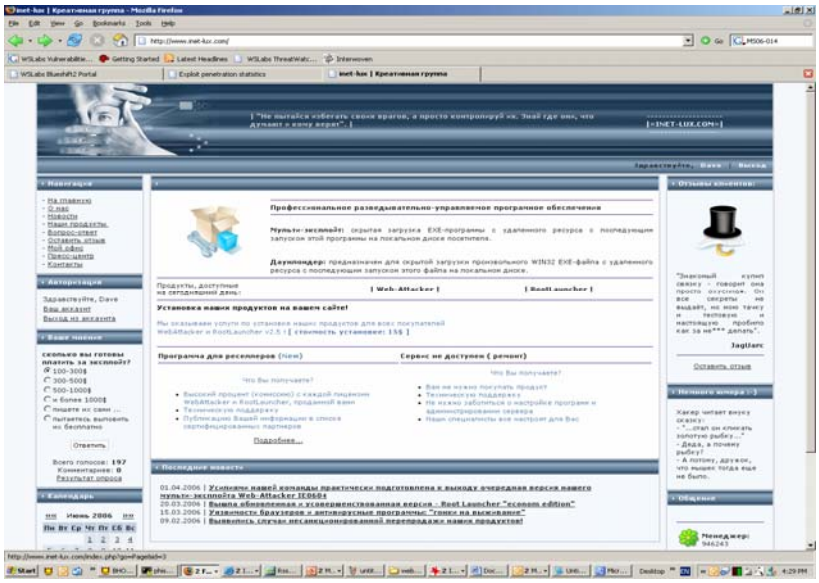
The kit includes a graphical interface and an instructional manual to assist in configuring the purchaser's server for the exploit. Along with that are details about which AV engines cannot detect it, and how it works.

The kit has the ability to detect the visiting user's browser through the user agent and serves one of seven different exploits based on the browser settings. It includes exploits for a number of different browsers and browser versions.

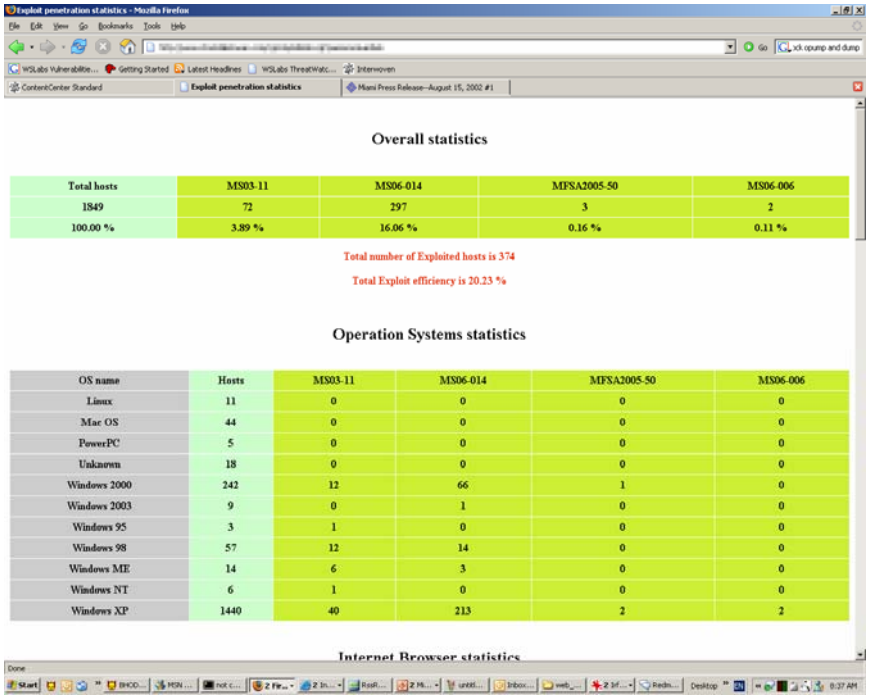
This toolkit can be purchased for $25–$300 and is widely deployed and used; at the end of the first half of 2006, we had 7,500 sites in our database that were using or pointing to WebAttacker code. The websites that are hosting the malicious code also include a statistics page that shows the number of infected clients, the percentage of clients that have been infected, and a breakdown by country, operating system, and browser. Recent statistics show very high infection rates with the newest version (approximately 12%–20%).

"Advertisement" for WebAttacker (translated from Russian) that appears on their site

Dear Friends! We would like to offer you multi-component exploit Web-Attacker IE604, that realizes vulnerabilities in the internet browsers Internet Explorer and Mozilla Firefox. With the help of this exploit you will be able to install any programs on the local disks of visitors of your web pages. In the foundation of work of the exploit Web-Attacker IE0604, there are 7 already-known vulnerabilities in the internet browsers: Objective of the Exploit: Hidden drop of the executable from the deleted source to the local hard drive of the site visitor.



This is the site that sells the code.



Overall statistics

Total hosts	MS03-11	MS06-014	MFSA2005-50	MS06-006
1849	72	297	3	2
100.00 %	3.89 %	16.06 %	0.16 %	0.11 %

Total number of Exploited hosts is 374

Total Exploit efficiency is 20.23 %

Operation Systems statistics

OS name	Hosts	MS03-11	MS06-014	MFSA2005-50	MS06-006
Linux	11	0	0	0	0
Mac OS	44	0	0	0	0
PowerPC	5	0	0	0	0
Unknown	18	0	0	0	0
Windows 2000	242	12	66	1	0
Windows 2003	9	0	1	0	0
Windows 95	3	1	0	0	0
Windows 98	57	12	14	0	0
Windows ME	14	6	3	0	0
Windows NT	6	1	0	0	0
Windows XP	1440	40	213	2	2

Internet Browser statistics

The administration reporting screen for a site with code on it that is infecting visitors lists statistics on the efficacy of the exploit, including the percentage of users that have been exploited and how (i.e., through which vulnerability).

Nuclear Grabber

Another toolkit example is Nuclear Grabber, which allows an attacker to sit on a real banking site and grab data from electronic forms. Like WebAttacker, this tool is available on Russian websites. The cost of Nuclear Grabber is a hefty $3,000.

Peer-to-Peer, Instant Messaging, and Chat

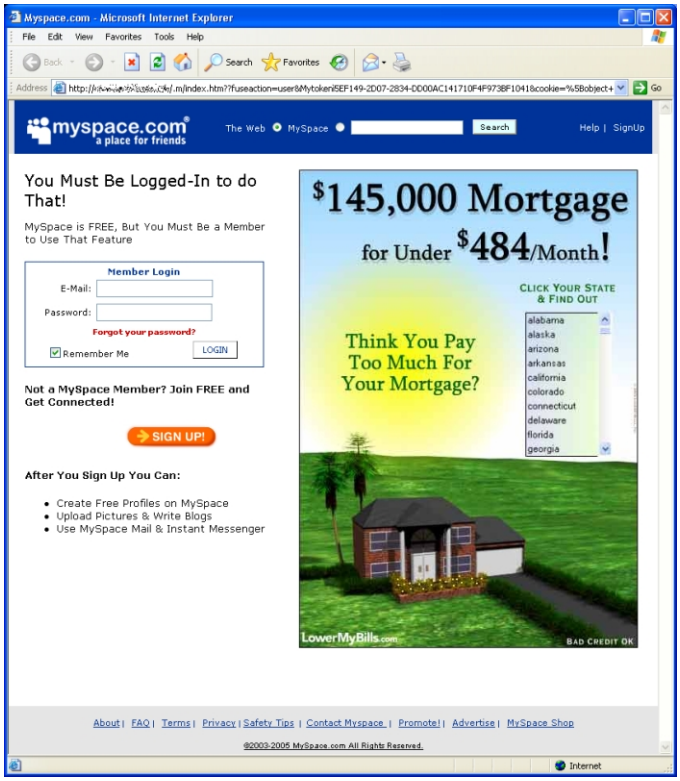
P2P botnets more difficult to shut down

Although the use of P2P itself to spread viruses remained about the same during H1 2006, we saw a change in the way P2P networks are used. Botnets are beginning to use P2P networks to gain control of more computers. Researchers were previously able to shut down a botnet by targeting its Command & Control center (and IRC channel or website). Hackers are now using P2P networks to connect bots in a more “horizontal,” peer manner, which makes shutting down the botnets much more difficult.

Myspace.com phishing attack

During H1, we discovered a phishing attack that attempts to steal account information of myspace.com users. A hyperlink is first delivered to victims via AOL Instant Messenger. Users who follow this link are taken to a fraudulent website that spoofs the myspace.com login page. This page captures their myspace.com account information and then forwards the users to the real myspace.com website.

The fraudulent site also sets a cookie on the victim's computer, which prevents the phishing attack from being displayed on any subsequent visits.



This spoofed myspace.com login page aims to capture myspace.com account information before forwarding the user to the real myspace.com website.

Websense Security Labs' Anti-Crime Efforts

Websense Security Labs continued to be at the forefront of the battle against crimeware. Websense Security Labs provided the research statistics for the Anti-Phishing Working Group's crimeware reports, and researchers presented findings at both APWG meetings and participated in the Crimeware "Petting Zoo" panels, where we presented latest examples of malicious code designed to steal information and exploit end users without their knowledge.

The Anti-Phishing Working Group defines crimeware as a genus of technology distinguished from adware, spyware, and malware by the fact that it is, by design, developed for the single purpose of animating a financial or business crime.

Project: Crimeware

During the first half of 2006, Websense Security Labs continued working with the Anti-Phishing Working Group (APWG) on Project: Crimeware, a program of collaborative research designed to capture, record, and characterize new and emerging incidents.

Research sharing and collaboration

During this period, Websense Security Labs continued to work with other researchers in the industry, organizations, and law enforcement with the goal of information sharing and collaboration. Bridging gaps between public and private sector and academia and commercial researchers is more important than ever as the criminal activity rises and the underground of attackers becomes more organized.

Projections for H2 2006 and Beyond

We expect to see increased use of social networks that link users. These networks allow people with common personal or professional interests to find each other easily. The linking of users or networks also gives attackers a method to attack multiple users through one entity or through a web of the network.

As the use of RSS (Really Simple Syndication) becomes more prevalent, today's software may not handle attacks well. Frequent updates of RSS, along with the embedding of downloads and encoding through a variety of XML formats, can lead to undetected infections.

As more applications become embedded within browsers (for example, a spreadsheet program that can be loaded within the browser), the web will become more of an application platform, leading to more opportunities for security vulnerabilities and problems.

The use of "underground" business tools will also increase. We will see the types and availability of certain types of toolkits – such as those for vulnerability testing – getting better, which bodes well for both researcher and criminal. For example, new technology – fuzzers – can automatically run a series of tests (millions of tests) against an application, searching for errors in the code. This technology will help researchers correct these vulnerabilities. These efficient tools in the wrong hands, however, can also help criminals find easy targets for their exploits.

The blackhat and whitehat markets for zero-day threats will increase, and the number of entities offering "rewards" to researchers who find and report vulnerabilities will likewise also increase. We will also see increased organization, sharing, trading, and commerce in the underground with regards to zero-day exploit code.

We will see more and more privacy issues connected to storage of personal, private, and confidential business data on the internet. As more and more people use the internet, more goods and services transactions will take place over the web (renewing vehicle registration, signing up for services, buying goods from web-based businesses, for example). As this happens, the danger of leaking data increases. For example, many companies offer 2GB of free personal storage space. People use this space to store resumes, letters, photos, passwords – all kinds of things. As people begin to store more business-related items, the threat to the enterprise will increase as well.

These online filing cabinets can store potentially sensitive personal and business information, which is very valuable and tempting to the cyber-criminal.

As additional compliance laws govern public disclosure of information breaches, we will see larger companies and organizations having to disclose attacks that could endanger their employees' and customers' information. In addition, as seen in the AOL search phrase web posting, users will have to become more aware of the amount of data that they are disclosing about themselves and their companies when using the web. Anonymity on the web will become more important than ever.

We will see increased use of P2P networks like Myspace and Linkedin to spread malicious code. This relationship vector, which allows us to connect to multiple people the world over, will also enable malicious code to spread more easily to friends, coworkers, and associates, increasing the global reach of worms, viruses, and other malicious code.

We will see increasing security concerns in the use of new entertainment technology. Web-enabling these technologies makes them an even greater target for miscreants.

Mobile attacks that use proximity (usually through Bluetooth) will also continue to rise. In the near future, these types of attacks will not have the impact they ultimately will in the longer term. However, the risk will grow as more mobile technologies are converted to "smart" phones, more become internet enabled, and as more information is stored on them.

About Websense Security Labs

Websense Security Labs focuses on areas such as malicious websites, phishing-based attacks, and other emerging threats associated with keylogging, spyware, instant messaging attachments, and corporate use of peer-to-peer applications. Websense Security Labs mines and analyzes over 85 million sites daily for malicious mobile code (MMC) and hacks. The team manages a honeynet of unprotected computers to discover new MMC, Trojan horses, keyloggers, and blended threats. The findings are used to study their techniques, actions, and behavior on an enterprise network system. Information gained from the network of honeypots provides valuable information that enables Websense Security Labs to discover attacks quickly and deliver remedies to Websense customers before antivirus signatures are available, thus closing critical opportunities for exposure. With this early detection system in place, Websense is able to provide a high degree of protection against rogue applications and new viruses to its customers, while also providing the security community with a much-needed resource.