WEBSENSE® Security Labs™

First Half 2005

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 2005 and presents projections for the upcoming period.

Contents

Introduction

About Websense Security Labs

Websense Security Labs™ was introduced in August 2004, with the primary objective of discovering and investigating today's advanced internet threats, and then publishing those findings. With extensive internet and malicious code categorization expertise, Websense Security Labs provides research and delivers timely product and information updates to the security community and Websense customers to support them in making their infrastructures more secure.

Like our previous report, this report summarizes significant findings during this period. This report also evaluates these threats in terms of trends and, where possible, also includes projections for the upcoming year.

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

Phishing	
Phishing emails	
Phishing keyloggers	
Phishing redirectors	
Pharming	
Malicious Websites	
Social engineering / deception techniques	
Keyloggers	
Toxic blogs	
Malicious Code	
Spyware – keyloggers	
Spyware – industrial espionage	
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	

The First Half of 2005 in Brief

The web as an attack vector continued to evolve and grow in the first half of 2005. We saw a marked increase in the number of malicious websites and in the amount of malicious code written with criminal intent ("crimeware"). The phishing landscape also changed considerably, with significant differences in the types of targets and types of attacks.

We also saw a change in how spyware is being used, with increasing use of keyloggers and screen scrapers in acts of industrial espionage.

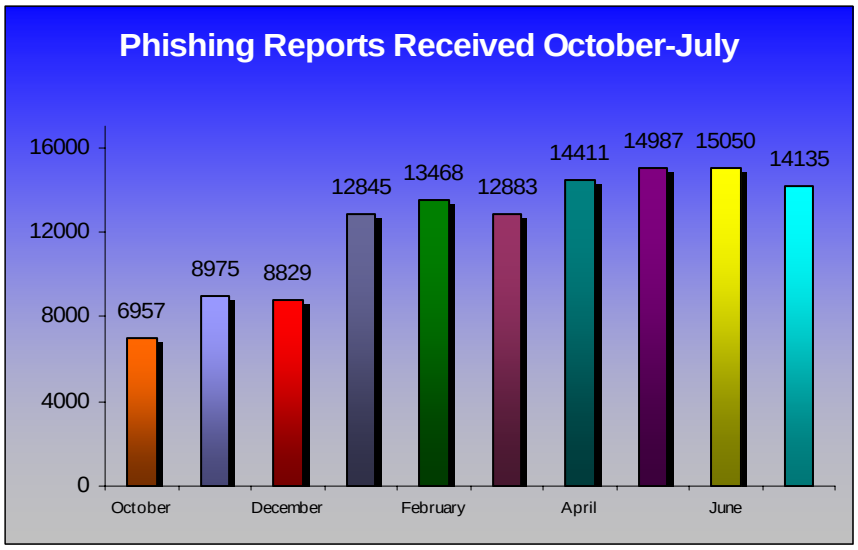
In the first half of 2005, Websense Security Labs was successful in identifying and hindering several high-profile exploits, including one aimed at MSN Korea. We also discovered a new type of attack — cyber extortion — in which money is requested from users to fix the very problem created by the cyber criminal.

Phishing

New targets, new types, and increases in international numbers

The attack landscape changed considerably during this period, with new targets and types of phishes. We also observed increases in the number of international brands targeted. We have also seen dramatic increases in the number of smaller, regional banks being targeted — credit unions, in particular. We have seen a growing number of small credit unions targeted by "puddle phishing" scams — more than 30 since the beginning of the year. Interestingly, at least one of the community banks recently targeted operates with as few as 11 branches.

Phishing is a method where information such as account numbers, usernames, and passwords is collected from users and then used to compromise their online accounts.



Courtesy Anti-Phishing Working Group

Focus on new targets

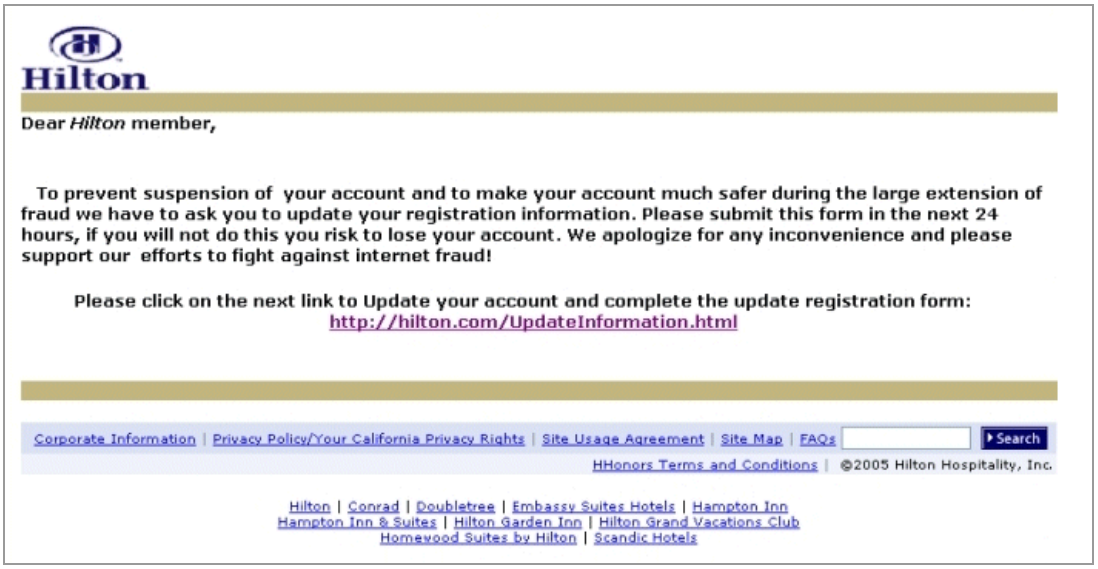
Although the numbers of phishing attacks are declining and the pace is flattening, we are seeing some trends in the types of targets that are being sought out. Many attacks in the first half of 2005 targeted non-financial-based organizations in the entertainment and games industries.

Some recent examples include Hilton Honors, Monster.com, and World of WarCraft.

The Monster.com and Hilton Honors Club attacks are examples of how phishing attacks have become more targeted. In both cases, specific user-accounts were profiled and lures appeared to have been sent to profiled accounts. Attacking specific corporations is also something new, where a lure is sent within a specific company in order to garner specific information. These attacks show that, when an attacker can profile or hone an attack, it can become that much more accurate.

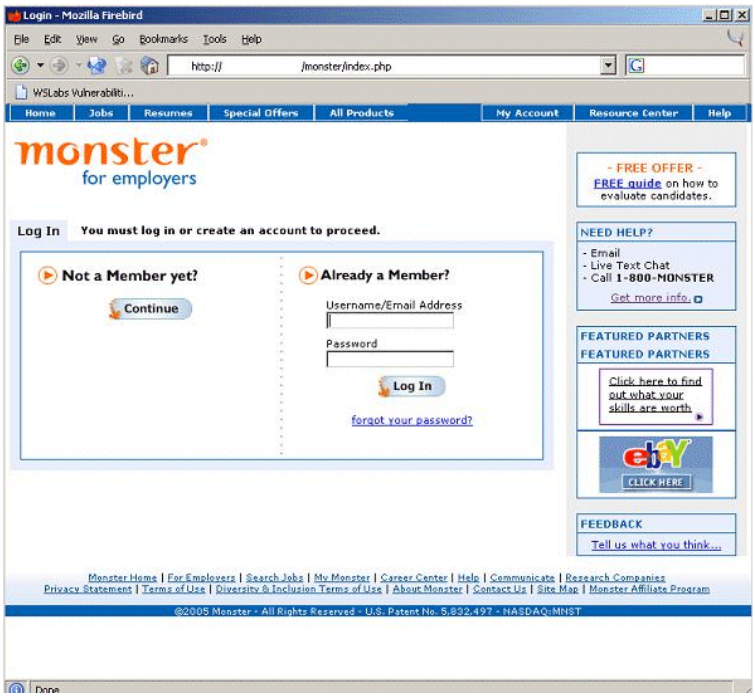
Hilton Honors Club attack

In this attack, members of the Hilton Honors Club receive a spoofed email message asking them to click a link to verify account information and help prevent internet fraud. If the users click the link, they are directed to a phishing site where they are instructed to complete a form requiring contact and credit card information. This site uses java script to attempt to spoof the browser address bar.



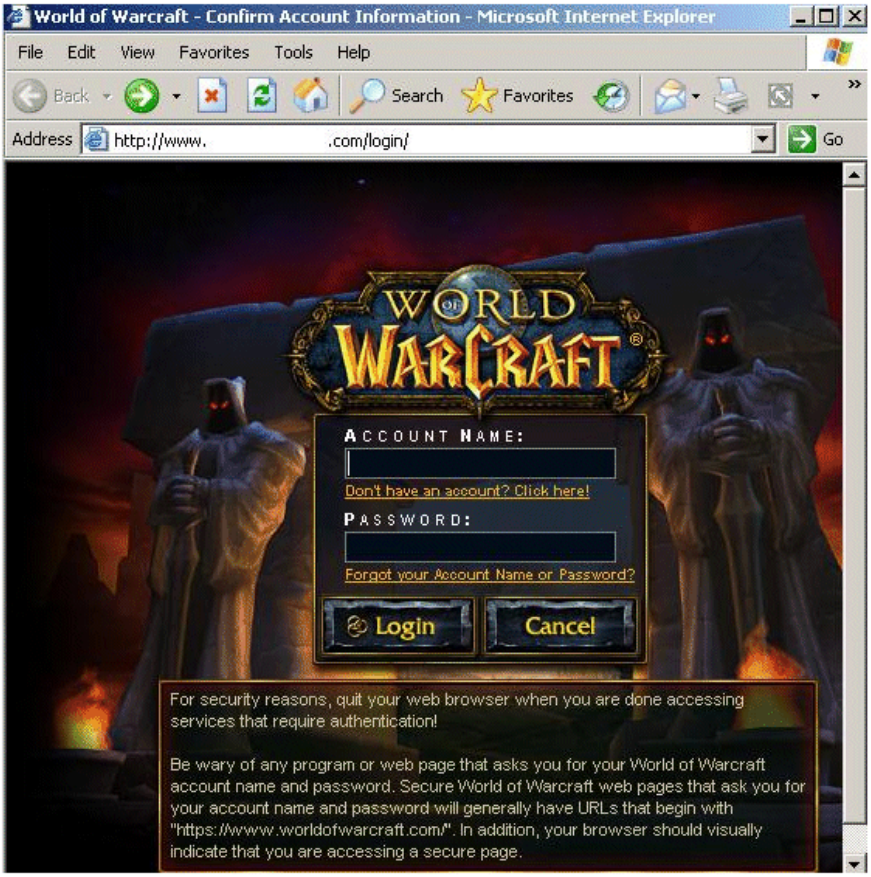
Monster.com attack

This phishing attack targets companies who use the Monster.com Employers section. In this attack, customers receive a spoofed email from the Monster Customer Support department informing them that their account has been suspended and that they must log in to validate their information.



World of WarCraft attack

Another fraudulent website targets users of the popular multiplayer online game, World of WarCraft. The site uses a cousin URL which is one character off the real website's address. When users access the fraudulent site, they are requested to log on to the system to play. When they enter their credentials, the information is then posted to the fraudulent website. The site also uses links and graphics from the real websites.



Puddle phishing

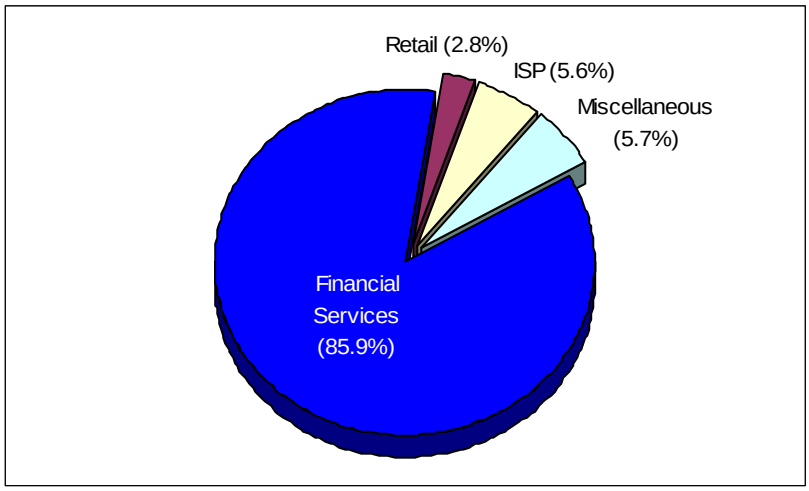
In the past, phishers focused on mainstream consumer websites with millions of users. Now the targets are becoming much smaller and more localized. By targeting a bank with just a few branches, the number of potential phishing prey is reduced to a much smaller number, sometimes to just a few thousand people. Nonetheless, the fact that we are seeing more and more of the smaller financial outlets being targeted by phishing attacks may indicate that this is a highly profitable scam.

Although the smaller size of the financial institution being targeted is a new phenomenon, the phishing method used by the attackers has not changed. The typical phishing email is still delivered as if it was from a legitimate financial institution and contains a message threatening to deactivate, block, or restrict users' accounts in some way if they do not update their personal account information. Users are instructed to visit a specific website, where they are prompted to enter confidential information such as ATM PINs, credit card numbers, Social Security Numbers, and email addresses.

The attack style and dynamics are very similar on many of these recent puddle phishing attempts, which may mean that there is some tool sharing or a small number of attackers behind this recent wave.

Summary of phishing targets

The most targeted industry sector for phishing attacks continues to be financial services, from the perspective of total number of unique phishing sites as well as the number of companies targeted. The financial services sector accounted for nearly 86%. This category includes phishing attacks against community banks and credit unions, in addition to well-known institutions with global brands.



Courtesy Anti-Phishing Working Group

Changes in types of phishes

In our 2004 report, we noted the ways criminals had begun to attack unsuspecting users in order to steal consumer information. Although phishing with social engineering lure emails and counterfeit websites is still the most prominent phishing technique, there has been a rise in the

number alternative methods used to co-opt consumers' online credentials or gain control of their accounts without using direct deception.

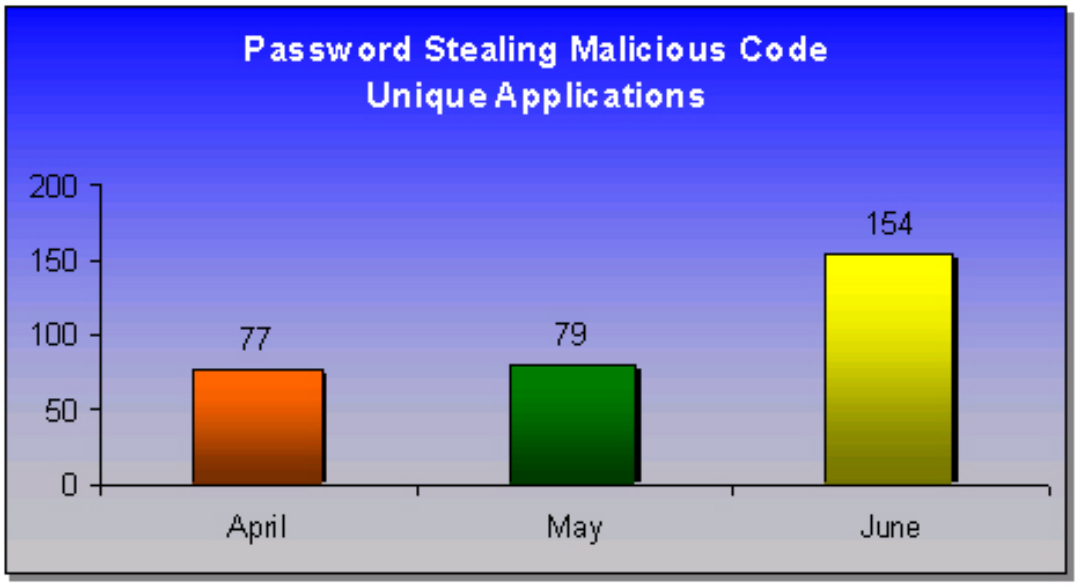
Trojan-type phishing system

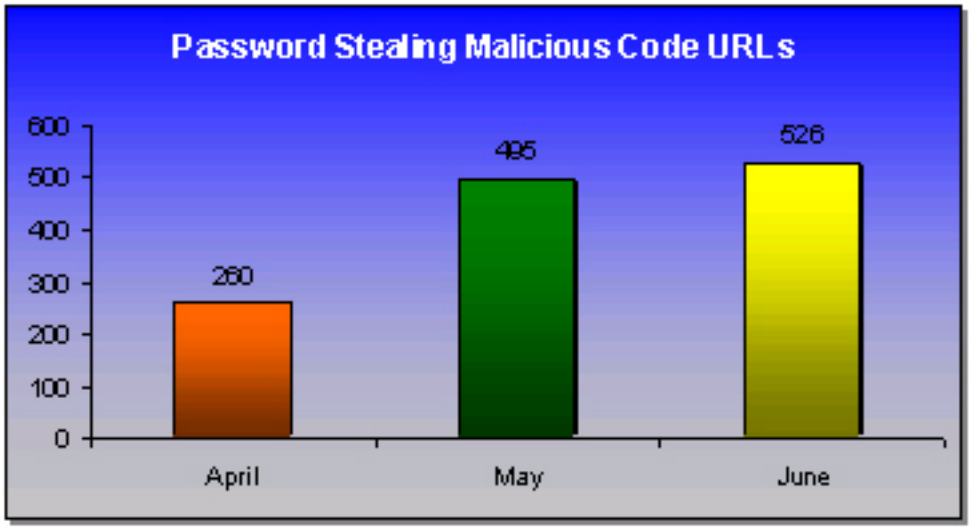
During this period, several Trojan horse keylogger attacks fully exploited the main advantage that this type of crimeware has when compared to traditional phishing. The attacks include a list of thousands of brandholders' domains, demonstrating the advance of phishing technology using wide-scope consumer-credential capture techniques. This finding indicates a drive by phishers to launch a generic keylogger attack against all credible, potential targets. Keyloggers were designed to log information when visiting popular financial institution sites, ecommerce and sales force portals, and even the online entertainment industry.

Phishing-based Trojans — Keyloggers

Unlike most generic keyloggers, phishing-based keyloggers have tracking components, which attempt to monitor specific actions (and specific organizations) in order to target specific information. The most common keyloggers seek access to financial-based websites, ecommerce sites, and web-based mail sites.

As the figures below show, we have seen an increase in the number of keylogging applications and the sites that host them.





Phishing-based Trojans — Redirectors

Redirectors transfer end user network traffic to a location other than that which the user intended. The "redirector" category includes crimeware that changes host files and other DNS specific information, browser-helper-objects that redirect information to fraudulent sites, and crimeware that may install a network level driver or filter to redirect to fraudulent locations. All of these are installed with the intention of compromising information, which could lead to identity theft or other credentials being taken with criminal intent.

We have seen an increase in the number of redirectors. The two most common are (1) Browser Helper Objects (BHOs), which are designed as browser plug-ins and redirect HTTP traffic to a fraudulent website instead of the intended destination, and (2) the modification of local DNS settings. By changing the hosts file and/or the DNS server settings, the destination can also be spoofed by redirecting the users to a fraudulent site.

Man-in-the-middle phishing — Pharming

Pharming is an attack that intercepts information between two parties' communications in order to redirect users to a fraudulent location. The most popular attack is DNS cache poisoning.

Other

Other recent examples include typo-attacks, where users mistype a popular domain and are then infected with crimeware, and search-engine poisoning, where users are directed to a fraudulent website, which downloads crimeware onto machines when users use a search engine.

Increases in international numbers

We witnessed significant increases in the number of international brands being targeted within their own regions.

During the reported timeframe there were large increases in phishing attacks against brands that are outside the U.S. and the U.K. Compared to H1 2004, where we saw five new target brands outside of the US and UK, during this period we saw more than 25 new attacks against brands from the following countries: Mexico, Japan, Spain, Italy, France, Dubai, Brazil, and Australia.

Reasons for changes and projections for the future

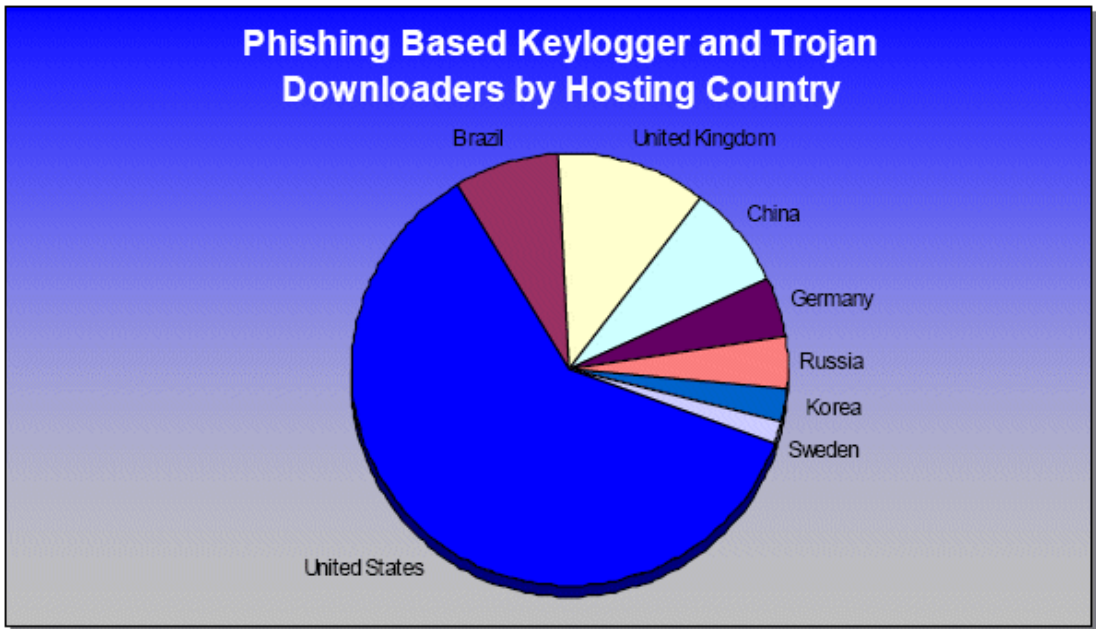
We believe that changes in the phishing landscape are due in part to the countermeasures and increases in end user awareness put in place by large financial institutions and ecommerce organizations. In response to successful counterattack measures, the attackers are setting their sights on other targets and changing their tactics.

Attacks are also becoming more sophisticated and difficult to detect. As banks and other organizations deploy more sophisticated anti-keylogging and other robust authentication methods, attackers will respond with new, more intricate approaches. The cat and mouse game will continue, and new attacks will evolve as defenses become stronger.

We also believe that there will be continued "hunting in packs," where criminal groups will share tools to create large-volume attacks with similar attack characteristics. Criminals will be able to leverage attack components and simply modify their targets.

H1 2005 phishing statistics

As the illustration below shows, the U.S. is still the top country for hosting phishing sites, with almost 55%. The U.K. is second with 10%, and Brazil is third with almost 8%. To date, Brazil still has the highest concentration of phishing-based keyloggers that target Brazilian financial institutions and use deception techniques written in Portuguese. Also, unlike regular phishing websites, phishing keylogger sites are not commonly hosted on compromised machines. It is more likely for them to be on a free hosting ISP, blog, or personal storage.



Malicious Websites

Capitalizing on software vulnerabilities and human nature vulnerabilities

As in 2004, we saw several software vulnerabilities disclosed in H1 2005 and followed shortly thereafter by exploits. However, we also saw an increase in the number of exploits against Firefox, in order to spoof the browser toolbar and others.

Malicious websites are sites that contain code that may intentionally modify end users' systems without their consent, causing harm.

Even though several browser vulnerabilities were exploited, traditional deception through social engineering is still the method used most often to infect end users with malicious code. Well-crafted emails, instant messages, and a variety of other devious methods are still being used to entice users to visit websites in order to infect them. These methods are often combined with vulnerability exploits; however, in most cases an executable sits on a website waiting for an end user to run it so it can work. The web is by far the fastest growing attack vector.

The motive for creating malicious websites is also trending away from annoyances such as changing the default homepage and adding bookmarks to a browser to more nefarious purposes like running exploit code to open a backdoor and changing browser address bars to fake banking and other sites for phishing.

MSN Spoof

Websense Security Labs received several reports of two new versions of spoofed emails that are being used to install spyware/adware onto users' machines.

The first version of the email claims to be from Microsoft®'s security department. It offers users a new security tool to help them feel more secure. The email points to an URL, which is hosted in Romania and was up at the time we issued an alert. Once the user accesses the site in Romania, a Microsoft Internet Explorer BHO DLL is then installed on the machine. This BHO is spyware.

----- Original Message -----
From: security@microsoft.com
<mailto:security@microsoft.com>
Subject: Microsoft Windows Update

Dear Windows
User,

Thank you for using Windows. Microsoft is constantly improving and we are trying to take care of your security. We offer you now a new security tool in order to feel more secure on the web.

Please click here <removed URL/MSUpdate.exe>
to install it.

Sincerely,

Microsoft Security TEAM

The second version claims that, because many people are illegally using its services without paying, Microsoft is requiring users to update their credit card information. The message reassures users that they will not be charged for any additional services at this time. The email links to a website which, when accessed, attempts to install a Browser Helper Object (BHO DLL) on the machine. The BHO is also spyware.

: Hello Microsoft user,

We here at Microsoft would like you to still receive your normal computer updates, That Will protect your computer from Viruses and spyware. We have noticed A lot of people are illegally Using our services Without paying for their Windows Operating System. Therefor we've made a web site so you can update or validate your windows serial and credit card information. If you do not comply with our policy, windows will ask you to reactivate your serial number, and it will become invalid.

So you will lose any information on your computer. If you do not validate your serial number, your copy of windows will be labeled as piracy.

Your Credit Card will not be charged. We use your credit card information to validate your windows system. If any one else has your serial number we will contact you by phone.

It is critical that you update your serial number and validate it, so no one else will attempt to use it. We've also added Programs to help fight

piracy and adware.

After your verification is complete, You can download these programs free of charge.

Please validate your account by Signing in our web site below.

<Site Removed>

Thank you

Removed
Windows XP Activation Team

Increases in Brazilian Trojan keyloggers

In early 2005, Websense Security Labs saw a dramatic increase in the volume of phishing-based malicious code — in particular, code that targets Brazilians. This code is designed to run on a machine and log keystrokes when a connection is made to predetermined websites. The keylogger then sends that information to a remote location for the purpose of identity theft.

From November of 2004 through December 2004, Websense Security Labs researched and identified an average of 1-2 new phishing keylogger variants and 10-15 new malicious websites hosting this code per week.

From February 2005 until now, we are researching and identifying 8-10 new keylogger variants and more than 100 malicious websites that are hosting these keyloggers per week.

Toxic Blogs release

Blogs are increasingly being exploited as a means to distribute malicious code and keylogging software. To date in 2005, we have discovered hundreds of instances of blogs involved in the storage and delivery of harmful code.

Cyber-criminals are now taking advantage of blog sites that allow users to easily publish their own web pages at no cost. Blogs can be attractive vehicles for hackers for several reasons: blogs offer large amounts of free storage, they do not require any identity authentication to post information, and most blog hosting facilities do not provide antivirus protection for posted files.

In some cases, the culprits create a blog on a legitimate host site, post viral code or keylogging software to the page, and attract traffic to the toxic blog by sending a link through spam email or instant messaging (IM) to a large number of recipients. In other cases, the blog can be used as a storage mechanism, which keeps malicious code that can be accessed by a Trojan horse that has already been hidden on the user's computer.

For example, on March 23, 2005, Websense Security Labs issued an alert detailing a spoofed email message that attempted to redirect users to a malicious blog. The blog would then run a Trojan horse designed to steal banking passwords. In this situation, the user received a message spoofed from a popular messaging service, offering a new version of their IM program. Upon clicking the link, the user was redirected to a blog page that was hosting a password-stealing keylogger. When predetermined

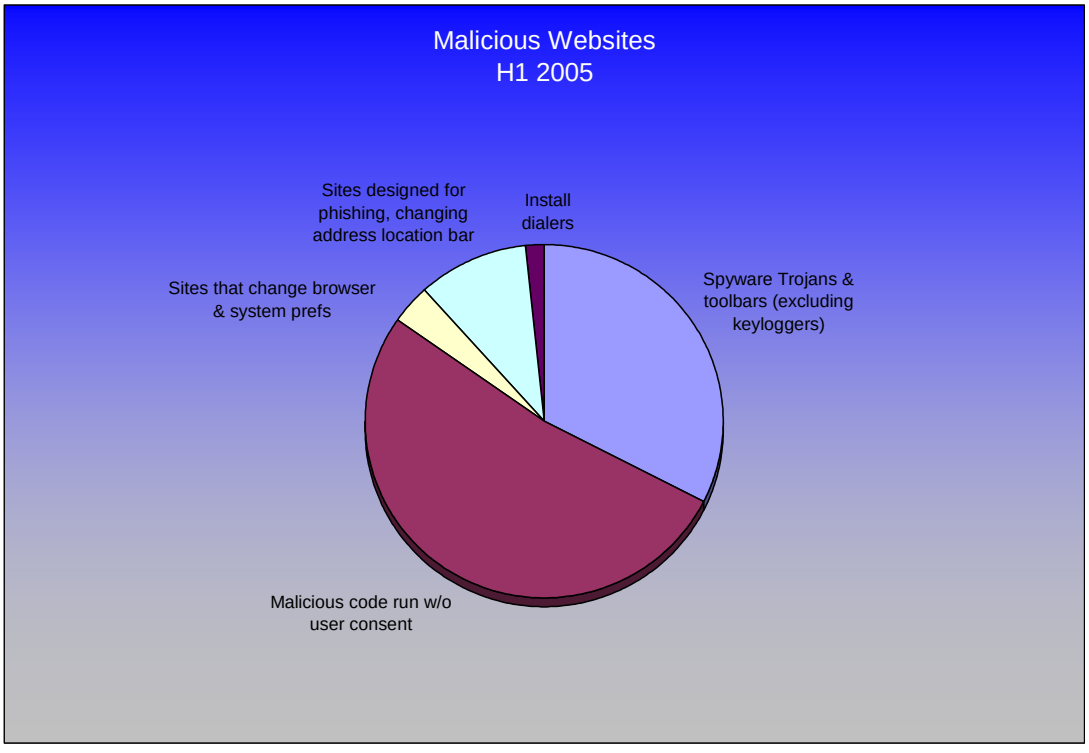
banking websites were accessed, the keylogger (bancos.ju) logged keystrokes and sent them to a third party.

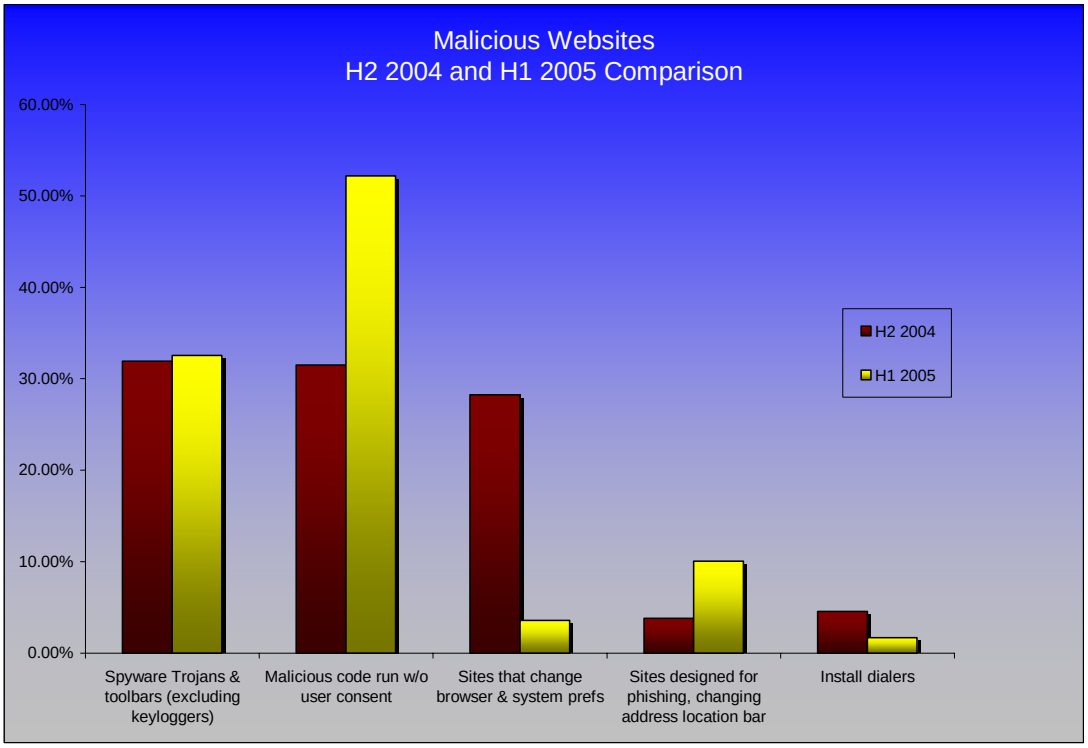
These aren't the kind of blog websites that someone would stumble upon and infect their machine accidentally. The success of these attacks relies upon a certain level of social engineering to persuade the individual to click on the link. In addition, the blogs are being utilized as the first step of a multi-layered attack that could also involve a spoofed email, Trojan horse, or keylogger.

Free personal storage sites

Free personal web hosting sites are increasingly being exploited by hackers seeking affordable and anonymous ways to store and disseminate mobile malicious code (MMC) and dangerous types of spyware, such as keyloggers, which are designed to steal personal and confidential information. Since the beginning of 2005, we have discovered more than 2,500 incidents of these websites distributing MMC, Trojan horses, and keyloggers.

H1 2005 malicious websites statistics




Malicious Websites
H2 2004 and H1 2005 Comparison
60.00%
50.00%
40.00%
30.00%
20.00%
10.00%
0.00%
H2 2004
H1 2005
Spyware Trojans & toolbars (excluding keyloggers)
Malicious code run w/o user consent
Sites that change browser & system prefs
Sites designed for phishing, changing address location bar
Install dialers

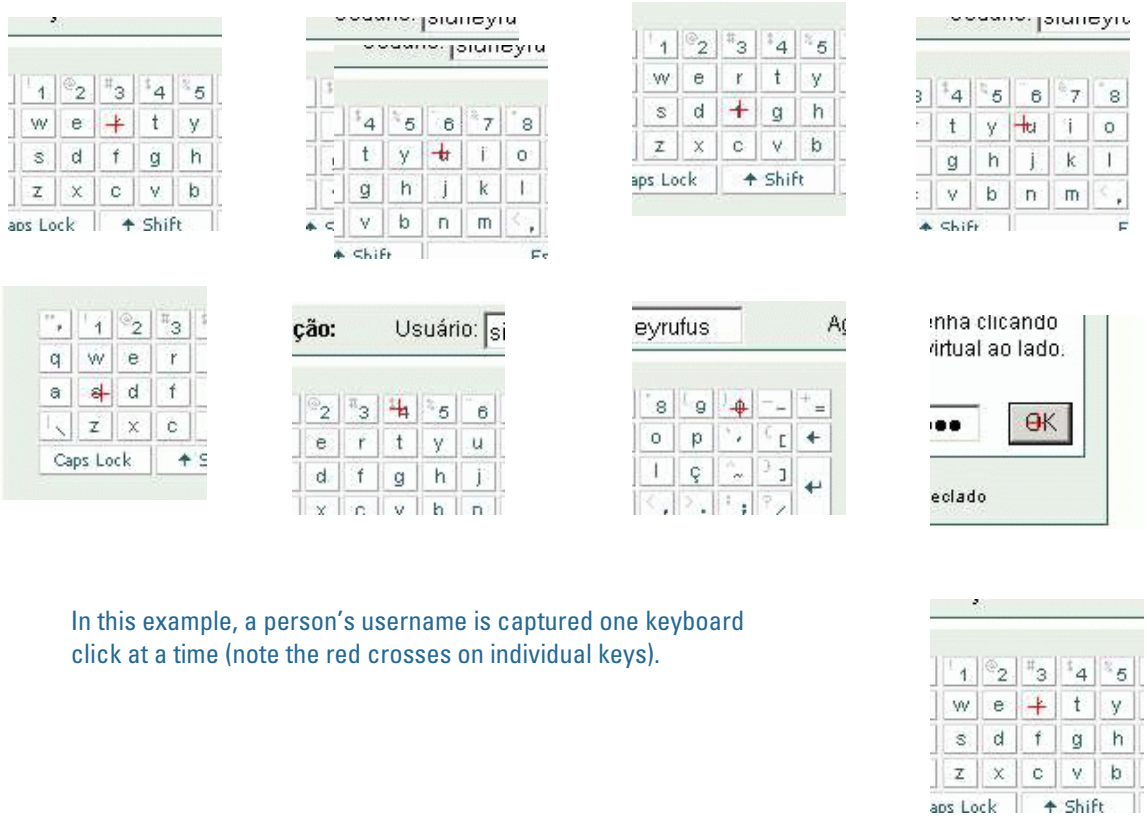
Malicious Code

Trojan horses, keyloggers, spyware, BOTs, and cyber extortion

The technology used last period to design standalone "Trojan horse" programs is now being used in phishing and spyware attacks. More and more we are seeing the distinctions between types of attacks becoming blurred, as cyber criminals combine techniques to accomplish their objectives.

Keyloggers and "screen scrapers"

During this period, we noted a new advanced spyware technique where HTML emails are sent to millions of users. Cyber-criminals use vulnerabilities in certain programs or use social engineering techniques to encourage users to run a program. When the program runs, mouse activity is captured a click at a time, and the results are then used to playback the clicks in order to capture the users credentials for the purpose of identity theft.



In this example, a person's username is captured one keyboard click at a time (note the red crosses on individual keys).

We also noted a case in the UK where the British Hi-Tech Crime Unit foiled what would have been one of the biggest computer crimes in history. Thieves attempted to transfer $420 million from a branch of the Japanese bank Sumitomo Mitsui. It is alleged that the thieves hacked into the bank's computer systems using information gleaned from keyloggers.

In another incident, a series of emails containing a variety of Trojan horse programs designed to steal economic and financial information was sent to a number of UK government departments for approximately six months — since January 2005.

Industrial espionage

We noted several exploits where organizations commissioned the writing of Trojan horses, with the express purpose of stealing information from their competitors.

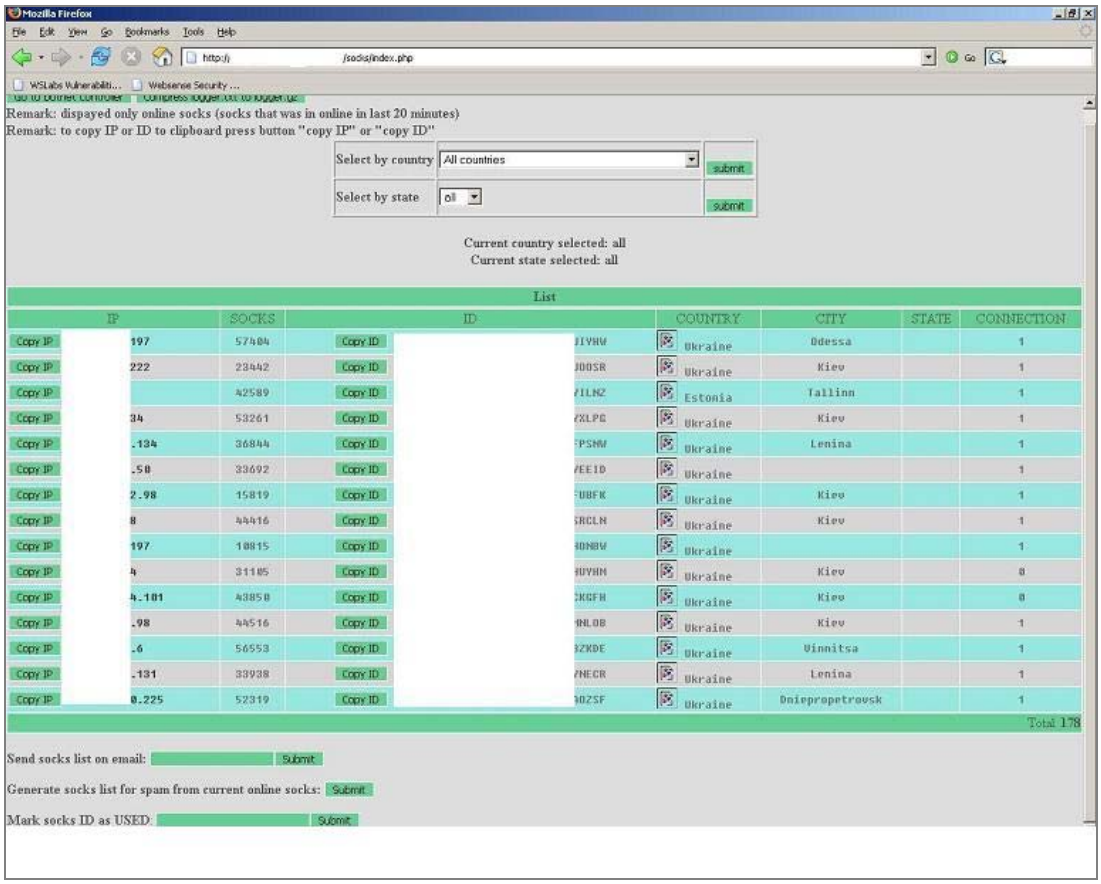
One example is Trojan.Hotword, in Israel. In this incident, a group of companies paid for the Trojan horse to be created. It was installed remotely, and thwarted desktop firewalls and antivirus software. This particular Trojan horse is self-updating, captures screen shots, sends emails, terminates processes, and executes new files.

BOTs

As with several other areas of malicious code, the cooperation of malicious code authors and spyware entities is resulting in increases in sophistication and in the numbers of machines that are infected. During the first half of 2005, we also witnessed an increase in the use of websites in order to control their "zombies" versus the more commonly use of Internet Relay Chat (IRC). This is particularly menacing, as most organizations filter IRC but do not filter HTTP traffic, potentially opening them up to BOT controllers via the Web.

A bot is a program (also called spider or crawler) that accesses websites and gathers content for search engine indexes.

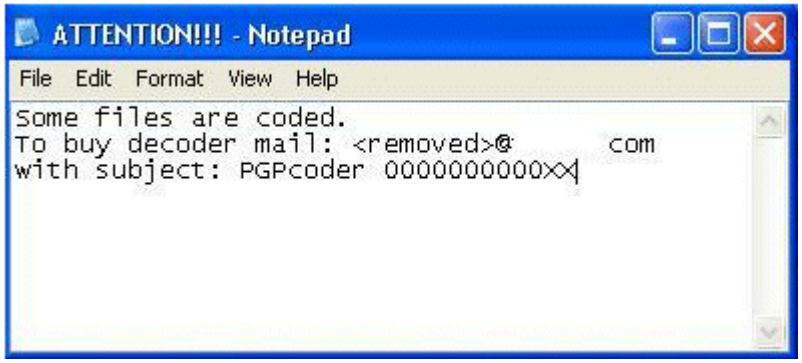
The screenshot below shows an example of a web-based controller where the infected zombies can be selected by region and then controlled through a single web interface. The attacker has complete management control of items such as poisoning the hosts file, running programs, capturing keystrokes, and installing new software on the machines — all remotely.



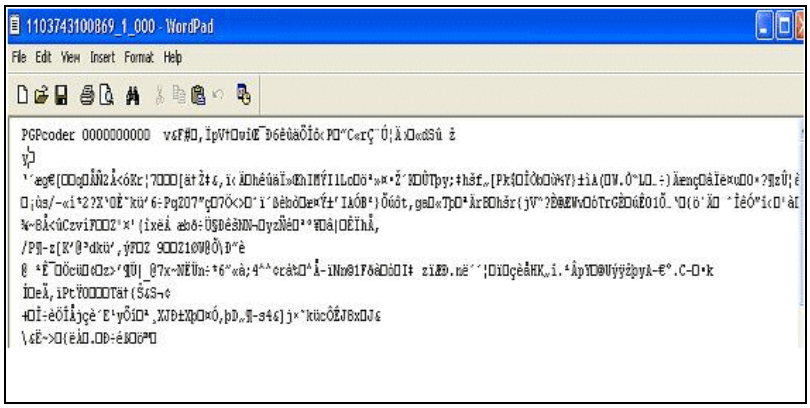
Cyber extortion discovery

In May 2005 we received reports of a new attack that attempts to extort money from users by encoding files on their machines and then requesting payment for a decoder tool.

The original infection occurs when the user visits a malicious website that exploits a previous vulnerability in Microsoft Internet Explorer. This vulnerability allows applications to run without user intervention. The malicious website uses the Windows help subsystem and a CHM file to download and run a Trojan horse (download-aag). The downloader then connects, via HTTP, to another malicious website. This website hosts the application that encodes files on the user's local hard disk and on any mapped drives on the machine. The malicious code also drops a message onto the system with instructions on how to buy the tool needed to decode the files. This message includes the email address of a third party to contact for instructions, and the user is directed to deposit money into an online E-Gold account.



In this screen shot, the user is informed that files are encoded and is provided with the URL to visit in order to buy the decoder.



This screen illustrates how encoded text appears to the user before it is decoded.

In this screen shot, the user is informed that files are encoded and is provided with the URL to visit in order to buy the decoder.

Spyware

H1 2005 spyware statistics

Some websites either host spyware-related downloads or are used as part of "back channel" communications. We saw the number of these sites increase by 285% from January 2005 to June 2005. During the same period, we saw the number of spyware-related applications increase by 373%.

Spyware evolution

The line between spyware and malicious code is blurring. Spyware authors are starting to employ similar techniques to get their

advertisements on desktops. The motives are also becoming more deviant.

Spyware classifications

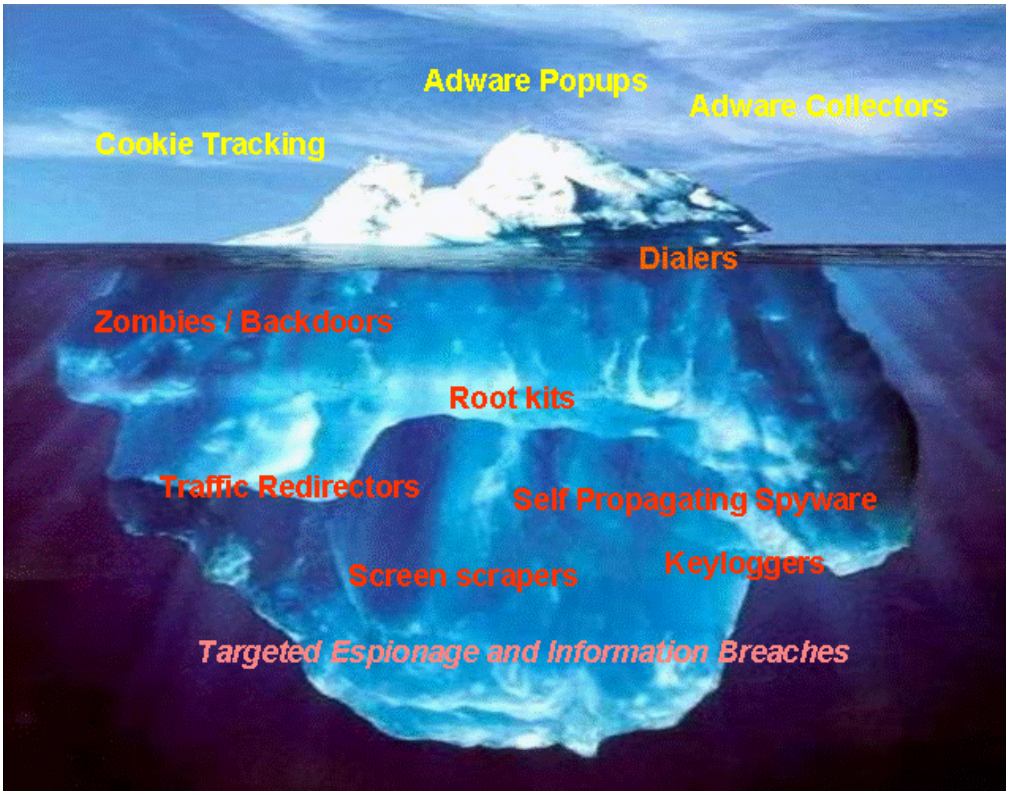
During the first half of 2005, Websense Security Labs joined the Anti-Spyware Coalition (ASC), a group dedicated to building a consensus about definitions and best practices in the debate surrounding spyware and other potentially unwanted technologies.

The ASC defines spyware as: Technologies implemented in ways that impair users' control over:

- Material changes that affect theiruser experience, privacy, or system security
- Use of their system resources, including what programs are installed on their computers
- Collection, use, and distribution on their personal or otherwise sensitive information

These are items that users will want to be informed about, and which the user, with appropriate authority from the owner of the system, should be able to easily remove or disable.

As the illustration below shows, several types of spyware fit this classification.



This illustration shows how spyware can be more than simply a vehicle to deliver advertisements to the end user. During the first half of 2005, several cases of corporate espionage that used targeted malicious code were used to gather information from banks and competitors.

Following the trend of other types of malicious code, the level of spyware sophistication has also risen. Code injection, DLL replacement, and rootkits are all being used to gain access to end users' machines. We are also seeing more difficulty in cleaning infected machines after the point of contamination. Code often modifies itself and the system over time in order to reinstall itself.

Hacking Websites and Hacking Tools

During the first half of 2005, several virus writers, spyware authors, and BOT controllers around the world were arrested. There appear to be more hackers for hire than ever, and a great deal of money is being made as more crime "professionals" have entered the arena. Hacking for fame is not as frequent as in the past; hacking for fortune is now much more common.

We also witnessed a case in Israel (mentioned previously) where prominent businesses were charged with hiring hackers to build a Trojan horse in order to spy on industry competitors. In the U.K., the Sumitomo Mitsui Bank barely escaped an illegal transfer of millions of dollars from a planned keylogger attack.

Hacking websites continue to be a place for trading and selling of information and tools to use for building your own malicious code or conducting a phishing attack. Credit card trading sites and identities are also being sold and bartered for online.

In this period, unique websites hosting hacking applications surpassed the 17,000 mark and hacking applications surpassed 10,000.

We project that increased cooperation and organization within the cyber-criminal underground will lead to more advanced techniques. In addition, the ability for criminals to monetize and launder the information they have is becoming more efficient.

Peer-to-Peer, Instant Messaging, and Chat

Throughout the first half of 2005, the use of the P2P networks, instant messaging, and chat have all increased as a means to distribute malicious code and entice users to visit malicious websites.

The BOT phenomenon of 2004 continued and attributed to most of the malicious code techniques that use P2P, chat, or instant messaging. Today more than 70% of the malicious code that uses one of the aforementioned attack vectors uses solely IRC. In most cases, IRC provides the means to command and control BOT networks (zombies).

Instant messaging was also used more frequently in attacks. Most of these attacks utilized vulnerabilities to spread or were combined with social engineering and a malicious website to entice the user to download and run code.

Microsoft Instant Messenger, AOL AIM, and Yahoo! were the favorite targets for malicious code writers.

The use of P2P in order to spread malicious code was flat through 2005. We saw no relevant increase or decrease from H2 2004.

Websense Security Labs' Anti-Crime Efforts

Project: Crimeware

In response to the increase in new types of phishing attacks using malicious code, Websense teamed with the Anti-Phishing Working Group (APWG) to create Project: Crimeware, a program of collaborative research designed to capture, record, and characterize incidents that are new and emerging. This new information will allow the APWG to include data in the monthly report and, possibly, other reports that specifically address the threats posed by crimeware.

The Anti-Phishing Working Group defines crimeware us 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.

Anti-Spyware Coalition

During this period, Websense Security Labs joined the Anti-Spyware Coalition (antispywarecoalition.org). This group, which was convened by the Center for Democracy and Technology, is dedicated to building a consensus about definitions and best practices in the debate surrounding spyware and other potentially unwanted technologies. Composed of anti-spyware software companies, academics, and consumer groups, the ASC seeks to bring together a diverse array of perspective on the problem of controlling spyware and other potentially unwanted technologies.

Conclusion

As organizations in the first half of the year adopted measures to fight phishing, we saw changes in the targets and types of phishing attacks launched during this period. We also saw increases in the number of international targets and in cases of puddle phishing.

With regard to malicious code and malicious websites, we saw continuing reliance on vulnerabilities in software and human nature. We saw increases in the u se of blogs and free personal storage sites to distribute malicious code and screen scrapers.

More keyloggers and screen scrapers were used in acts of industrial espionage, and we witnessed the first case on record of companies actually commissioning hackers to steal competitor information.

We saw a change in the way bots and zombies are controlled in this period: fewer used IRC and more used websites. We also witnessed cases of cyber extortion, where criminals demand payment for resolving problems they themselves created. The number of hacking websites and tools increased, and P2P networks, instant messaging, and chat continued to be used to distribute malicious code.

We believe that the number and type of attacks will continue to increase and evolve in the second half of 2005, resulting in more monetary gain for the attackers and damage to the victims. We also believe that, as organizations adopt methods to defend against attacks, cyber criminals will invent new ways to achieve their goals, even establishing coalitions to share tools and methods for even greater gains.

About Websense Security Labs

Websense Security Labs focuses on areas such as malicious web sites, 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 37 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 a remedy to Websense customers before antivirus signatures are available, thus closing a critical opportunity 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 providing the security community with a much-needed resource.