WEBSENSE® Security Labs™

Second Half 2004

Security Trends Report

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 second half of 2004 and presents projections for the upcoming year.

Contents

Introduction

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.

This report summarizes findings during the second half of 2004. 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

The rise of the cyber criminals

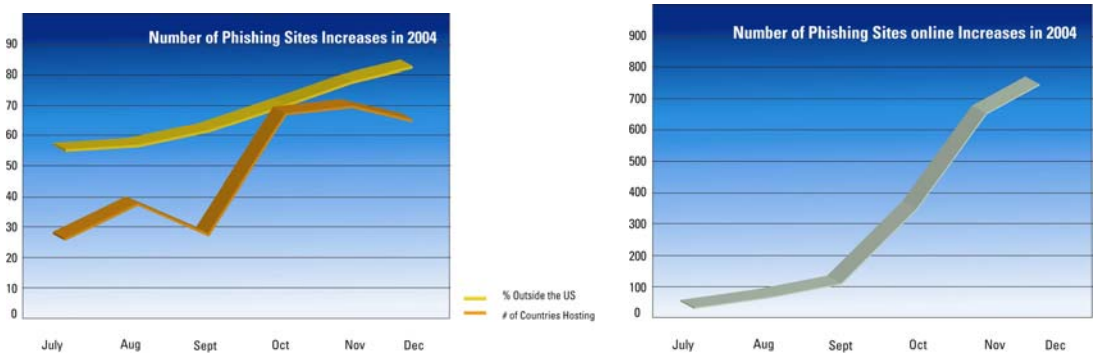
The second half of 2004 saw a dramatic rise in the quickly mounting and emerging threat of phishing.

> *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.*

Phishing has grown in number, frequency, and sophistication like no other security threat in the past. Although most phishing attacks target users of financial institutions, ISPs, and online ecommerce sites, we have seen attacks that seek out network username and password credentials, a potential sign that targeted attacks are on the way.

2004 phishing statistics

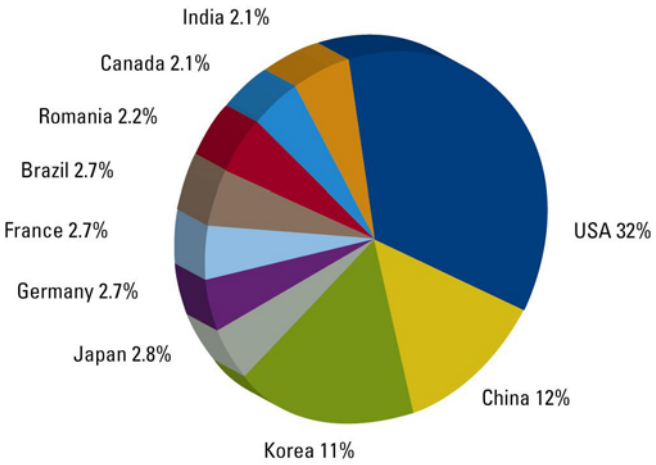
As the illustration below shows, the number of phishing sites rose dramatically in the second half of 2004. In fact, starting in October, the number of sites hosting phishing attacks nearly doubled overnight. The “phishers” appear to have become more organized and sophisticated, and the types of attacks also changed, with compromised PCs becoming the number one haven for hosting attacks.



The attacks also became more widespread geographically. In July, only 35 registered countries hosted phishing sites; in October, November, and December, we saw that number nearly double to 66. Although the U.S. is still the top country for hosting phishing sites, China and Korea gained in percentage each month, a fact

we attribute to the lack of governance and international law. The illustration that follows identifies the countries that are currently hosting phishing sites.

Countries Hosting Phishing Sites



More sophisticated phishing attacks

The sophistication of the attacks has also changed. Early phishing expeditions involved luring users with emails only, the text of which often contained misspelled words and broken links. Today's phishing attacks are accomplished through keylogging malicious code, instant messaging, and online chat rooms. Phishers are also using browser vulnerabilities to exploit users.

> *Phishing attack techniques are morphing—using browser and OS vulnerabilities to infect users with keylogging malicious code that monitors and tracks web surfing habits and other behaviors of the end user.*

At any one time there are more than 800 sites online, established with the sole objective of stealing information from users. Attacks typically move from location to location and are online for fewer than three days at a time.

Fraudulent websites on the rise

In the second half of 2004, we also saw a dramatic rise in the number of fraudulent websites. Much like phishing sites, fraud sites are set up to lure users into divulging confidential information for theft. However, unlike phishing, these sites do not target / advertise any particular products or brands. Instead, they pose as

online e-commerce sites that encourage users to apply for a reward or purchase something, of course never delivering on any of these promises. The most popular areas are online pharmacies, lottery scams, and loan / mortgage sites.

The future of phishing in 2005

Attacks that use browser vulnerabilities

As we move into 2005, we are seeing more phishing attacks that capitalize on vulnerabilities in browser technologies. Some examples include task bar replacements, address location bar replacements, domain names replaced with falsified information, ploys that use DHTML to display fake toolbars, and those that use several other vulnerabilities to run code on users' machines. We believe that search engines will be used as a ruse to trick users into connecting to phishing and fraud-based websites.

More fraudulent merchants

Along with the continuation of phishing attacks, we believe there will be a marked increase in the number of fake / fraudulent merchants, in new areas besides the familiar pharmaceuticals, online gaming / lottery, and loan mortgage scams.

More MMC that runs keyloggers

Phishing methods that use malicious code to run a keylogger on users' machines will also become more prevalent, as will the use of automated telephone scams and messages.

Malicious Websites

Zero-day exploits and the web as an attack vector

In the second half of 2004, we saw a number of high-level outbreaks that used the web as an attack vector in order to propagate malicious code.

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

Several cases were reported where users were infected with malicious code when they simply visited a website; these infections occurred without the user having to run any programs or open any attachments.

Although some sites rely on social engineering to download and install code, most use browser vulnerabilities or vulnerabilities within scripting languages' security enforcement, such as JavaScript, Active X, VB Scripts, and Java Applets.

During the year, dozens of web browser vulnerabilities were reported. In many cases, proof-of-concept (POC) code and examples were available on the internet for download. This, combined with the fact that patches did not exist for most of the vulnerabilities, led to many web-based exploits.

Starting in late June and moving into July, we saw a large outbreak of an attack that compromised several advertising network hosts in order to infect users. We also witnessed the rise of a dual-pronged attack, which used both web server and web browser vulnerabilities to launch malicious code on users' machines. Upon visiting infected websites, clients were invisibly redirected to a Russian web server, code was downloaded, and the end users' behavior was monitored to determine when well-known banking sites were visited. When the banking sites were visited, a keylogger sent the users' information to a remote website. The attack details were coined "download.ject" and "js/scob."

In August, another unpatched vulnerability within the browser was exploited, which utilized "drag and drop" functionality. This exploit resulted in several sites being compromised and a Trojan horse being spread to users' PCs. This attack was coined "Akak." During

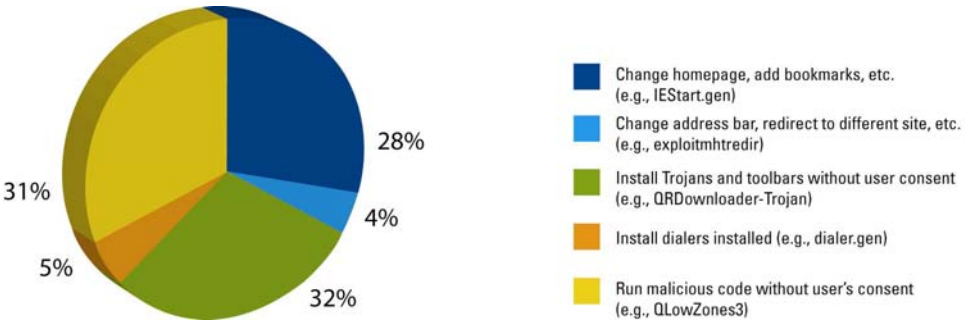
November, more sites were compromised, designed to install adware and Trojan horses when users visited them. We also tracked malcode called “Bofra,” which was distributed on some sites. Finally, in December, the “Phel” attack occurred, using a still-unpatched vulnerability in XP SP2 to download and launch a Trojan horse on end users’ machines.

2004 malicious websites statistics

Currently, tens of thousands of malicious websites are active on the internet. These sites fall into three main categories: (1) sites that are hosted and set up with malicious intent in mind, (2) sites owned by other people with a web server that has been compromised and set up as an attack point, and (3) broadband connected PCs which have been compromised and where a web server has been set up.

Malicious sites are hosting the following types of attacks:

- Sites that modify a user’s browser settings, bookmarks, homepage, and startup files.
- Sites that install adware and spyware on a user’s machine.
- Sites that install keyloggers on a user’s machine.
- Sites that install Trojan horses on a user’s machine.
- Sites that install dialers on a user’s machine.



The future of malicious websites in 2005

Web used for attacks

As more and more companies are stripping attachments from emails, the web will continue to rise as a popular attack method. Several vulnerabilities in the most popular browsers in the market remain unpatched today. We will continue to see vulnerabilities on the browser side and on the server side as well, with web server

technologies moving forward and proof of concept code (POC) easily available to exploit those vulnerabilities.

More zero-day exploits

In 2004, we saw zero-day exploits where users could be infected by simply visiting a website. In 2005, we will see more of these types of exploits. We also expect to see increased use of compromised broadband connected PCs, with the risk of higher-profile sites being used to spread malicious code, in addition to the advertising networks and other distributed sites.

Poisoning of search engine results

We also believe that an increase in “poisoning” search results from the most popular search engines is possible. In this scenario, attackers ensure that their sites appear high in the return lists of queries; when users visit those sites, they are infected. For example, in a search for “anti-spyware” a list of sites infected with spyware might actually top the list.

Web used in combination with other attack types

We expect the web will continue to be used in concert with other attack types. A good example is the BOT phenomenon, where attackers are starting to use the web along with other technologies such as internet relay chat to keep track of infected users and even control networks of infected machines.

Malicious Code

Trojan horses, keyloggers, spyware, and BOTs

Websense Security Labs researches many types of malicious code, including high-impact worms, spyware, advanced spyware (keyloggers), Trojan horses, and BOTs.

Spyware

Spyware problems continued in the latter part of 2004, with more media hype than ever before. In September, Websense Security Labs decided to divide spyware into two separate categories: spyware and keyloggers. This decision was based on customer input that the less nefarious adware should not gain the same amount of attention within logs as the more dangerous spyware, which in most cases is designed to log keystrokes and send them back to a third party.

Currently, we have logged more than 500 malicious keyloggers and more than 1,500 keyloggers that are commercially available.

BOTs and BOT networks

During 2004, we saw a significant increase in the number of BOT applications used to transform machines into BOT networks. The BOT networks were used for a number of reasons:

- SPAM relay
- Generic traffic proxies
- Distributed Denial of Service (DDOS) attacks
- Hosting phishing websites
- Hosting other malicious code websites

The motivation behind setting up BOT networks was in most cases a monetary one. BOT networks could be used to capture important, confidential user information which could then be sold or traded; the horsepower of the networks could be sold for spamming millions of users; and these BOT networks could be used to sell DDOS and / or extort companies with DDOS threats.

Trojan horses and keyloggers

During 2004, we saw large increases in the number of Trojan horses. Most of the high-impact worms, such as Netsky, Mydoom, Bofra, and others, used Trojan horses to enable backdoor access to the machines.

Along with Trojan horses, keyloggers also became a popular weapon of the blended threats arsenal. Primarily used to capture user credentials when visiting known websites, keyloggers grew in sophistication, adding behavior monitoring, web-surfing habit tracking, and their own SMTP and HTTP post engines.

We have also seen an increase in the number of commercial keyloggers that can be downloaded on the internet. These keyloggers typically advertise the following features:

- Installs remotely
- Bypasses firewalls and email scanning
- Not detected by antivirus
- Encrypts the keylogger content
- Captures all keystrokes and screenshots
- Captures the passwords behind the asterisks
- Sends email to remote sites undetected

These commercial keyloggers may be marketed as products that allow you to spy on your spouse or watch your children's online activities. They are often used as packaged attacks designed to capture keystrokes to gather online banking passwords, login credentials, Social Security Numbers and other identity-related information.

Spyware statistics

2004 spyware-related websites

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 almost 78% from August 2004 to January 2005.

2004 spyware-related applications

The number of applications also increased steadily in 2004, up about 52% from August to December. However, in January we saw a marked decrease, to approximately 5,400.

The future of malicious code in 2005

Improved delivery methods

The promise of increased monetary gain by attackers has resulted in a more sophisticated network of perpetrators and better organization among them. The threat of malicious code keyloggers and behavior-based malicious code that tracks surfing habits and potentially even correlates the habits to build profiles continues. However, we do not see much improvement in the sophistication of the design of the malicious code itself. Rather, the advancements are in the delivery methods and infection routines. Typical methods continue to be used to avoid antivirus product detection; however, attackers exploit flaws within browser vulnerabilities and the other weaknesses of today's technologies to gain access to hosts.

Combined technologies and locations

Malicious code attacks are increasingly combining several technologies and locations to thwart detection and investigation. Some recent examples include combining internet relay chat and the web in BOT attacks and using multiple compromised machines to host separate components of phishing and other fraudulent activity.

Hacking Websites and Hacking Tools

Blackhat hacking easier than ever

Simply search using any of the more popular search engines, and you'll find portals where hacking tips can be gathered, source code and hacking binaries can be downloaded, and discussion groups conversing about the latest techniques to thwart today's security mechanisms can be found. The attackers have the upper hand in this cat-and-mouse game and appear to have become much more organized in 2004, as evidenced by the increase in the number of online portals, hacking tools, and message groups.

As hacking sophistication has grown so has the availability of hacking tools and portals designed to assist in cyber attacks. While one could argue that the accessibility of these tools and portals helps both Whitehat and Blackhat hackers, they are often used as breeding grounds for malicious source code and other tools designed to breach information security. Password dictionaries, password crackers, viral source code, social engineering techniques, zero-day exploits, and backdoors into organizations' networks are all freely available on the internet.

We have also seen releases of source code for major viruses, which have led to several subsequent variant releases. As outlined in the Phishing section, as more monetary gain becomes available, so will tools and sharing of information in the security underground.

During the year, several browser vulnerabilities were reported with POCs, which may have led to the release of malcode by malicious attackers. It can be argued that this knowledge may help the companies in the security community as well, however.

The future of hacking websites and hacking tools in 2005

Better organized attackers

Never have attackers been more organized than they are today; we see this trend continuing into 2005. Along with popular chat protocols, the web will continue to be used as a popular means for trading tools, hosting discussion groups, and uploading other information.

More resources available

The sharing and selling of tools will also escalate. With so many exploits and POCs being released on the web, attackers now have a plethora of places where they can download the “latest and greatest” code to use and / or modify and use for their own purposes. All types of malicious code are freely available to download; continued source sharing and source code distribution will undoubtedly lead to more variants.

Although many of the hacking tools available are designed to help security professionals and are, in some cases, important arsenals in helping to protect organizations’ assets, they can be and are also used by other people with malicious intent.

Peer-to-Peer, Instant Messaging, and Chat

P2P, IM, and chat used as attack methods

As the use of peer-to-peer, instant messaging, and chat increases, so does the increased use of those technologies as an attack method. Throughout 2004 we saw blended malicious code attacks, which utilized the P2P networks and instant messaging as attack vectors.

P2P networks

In order for P2P clients to attract as many users as possible, they are now designed to circumvent firewall technology by using port 80, which is open in most organizations. Most clients today will attempt to connect with predefined ports and, if they are not available, will connect over port 80. Often the clients will mask their user-agents, disguising themselves as “Internet Explorer” or “Mozilla.” As more and more users are connecting to the P2P networks from work, the risks associated with the downloading of malicious code and illegal files are increasing.

Not only have P2P networks been utilized to host malicious code, they are also a “safe haven” for trading hacking tools and illegal copies of software, music, and movies.

Instant messaging

As with P2P, the use of instant messaging is rising dramatically. It has been predicted that IM will surpass email as the number one communication method on the internet. However, unlike email, IM in most companies is unregulated and bypasses security measures implemented to help protect companies. Both social engineering and vulnerabilities within client technologies are being used to gain access to hosts. In 2004, the most popular malicious use of IM was to send the user a link to a malicious website and / or a phishing or fraudulent site which then installed code, ran code, or duped the user into divulging confidential information.

As companies continue to add blanket restrictions on email attachments, attackers are utilizing the weaknesses in IM clients and the IM infrastructure itself. Most instant messaging protocols are designed to work through firewalls that have port 80 open,

often circumventing corporate security restrictions, acceptable use policies for mail, and gateway antivirus solutions.

Chat

Unlike instant messaging, chat protocols are not nearly as popular for most day-to-day users of the internet. However, chat in general and internet relay chat (IRC) in particular are very popular tools for attackers. IRC is used to control most BOT networks today and is also used to trade tools and discuss attacks, as well as other malicious reasons such as trading stolen credit cards, username and passwords, and malicious code samples.

Although web-based BOTs are becoming more prevalent, IRC remains to be the number one technology used to command and control large numbers of compromised computers connected to the internet (also referred to as BOT armies).

The future of P2P, instant messaging, and chat in 2005

P2P used to distribute MMC

We see a continued use of the P2P networks as a means to distribute malicious code.

Typical social engineering techniques will continue to be used to lure users to download what appear to be music and other media files. We also see an increase in the distribution of illegal copies of software and hacking/cracking tools on the P2P networks.

IM as an attack vector

We believe that instant messaging will be used more often as an attack vector in 2005, primarily as a means to get users to access a malicious website or to download and run malicious code. Instant messaging will continue to be used as a social engineering tool to gather information about users and their identities. The identity of users is often anonymous, and the very nature of real-time communications like instant messaging presents a new opportunity for acquiring this information. Exploiting existing and new vulnerabilities within instant messaging technologies will also rise.

New methods

Although IRC will continue to be used to control BOT networks and to discuss and trade attacking methods and tools, we believe that the release of new technologies and more coordinated efforts to prevent their use will lead attackers to alternate methods. These methods may or may not include the web, DNS, and P2P technologies to distribute and control the armies of compromised machines, and the use of the web.

Conclusion

As the potential for monetary gain increases, so will the sophistication of attacks. We believe attacks will evolve at a pace similar to those we witnessed in 2004; however, there will be more monetary gain – and damage. The attackers are becoming more organized with their technology trading and sharing, capitalizing on the lack of international law and governance, and using difficulties in tracing the attacks to their advantage. Attackers are also no longer relying solely on social engineering to accomplish their goals. Now they are cleverly using combinations of resources and techniques – exploiting browser and OS vulnerabilities and using the web and IRC to control BOT networks, etc., for example.

We believe that awareness and user education are critical, but also believe that, since many of the attacks rely so heavily on social engineering, the necessary understanding will only come after events occur.

Because of the increasing number of released vulnerabilities on popular browsers, operating systems, web servers, and other internet technologies and the decrease in time between reporting and exploiting those vulnerabilities, we believe the 2005 attacks will have significant monetary and productivity impacts on organizations and individuals.

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.