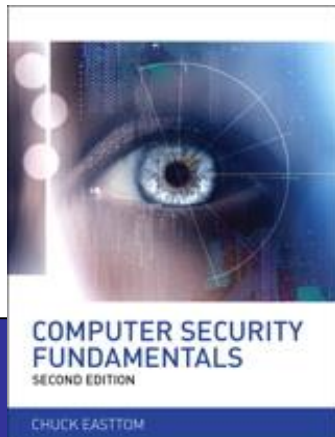


Computer Security Fundamentals

by Chuck Easttom



Chapter 5 Malware

Chapter 5 Objectives

- Understand viruses and how they propagate
- Have a working knowledge of several specific viruses
- Understand virus scanners
- Understand what a Trojan horse is

Chapter 5 Objectives (cont.)

- Have a working knowledge of several specific Trojan horse attacks
- Understand the buffer overflow attack
- Understand spyware
- Defend against these attacks

Introduction

- Virus outbreaks
 - How they work
 - Why they work
 - How they are deployed
- Buffer overflow attacks
- Spyware
- Other malware

Difference between IDS, IPS and Firewalls

- Lets compare an enterprise network to a financial institution.
- The security guards checking your ID and verifying your visit are the firewall.
- The cameras that alert the security guards that an unknown person is loitering near the vault room are the IDS.
- The automatic Gatling guns that open fire on an unauthorized person loitering near the vault room are the IPS.

Viruses

- A computer virus
 - Self-replicates
 - Spreads rapidly
 - May or may not have a malicious payload

I love you virus



Viruses (cont.)

How a virus spreads

- Finds a network connection; copies itself to other hosts on the network
 - Requires programming skill

OR

- Mails itself to everyone in host's address book
 - Requires less programming skill

How does malware spread?



Free
software



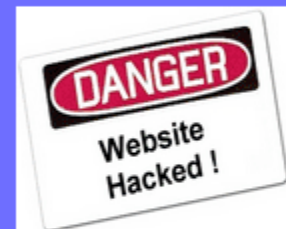
Suspicious
popup ads



Spam email
attachments



P2P sharing
files



Malicious
websites

Viruses (cont.)

- E-mail propagation
 - More common for one major reason;
 - Microsoft Outlook is easy to work with.
 - Five lines of code can cause Outlook to send e-mails covertly.
 - Other viruses spread using their own e-mail engine.

Viruses (cont.)

- Network propagation.
 - Less frequent, but just as effective
- Web site delivery.
 - Relies on end-user negligence
 - End user negligence

Recent virus examples

- www.f-secure.com/virus-info/virus-news/
- <http://securityresponse.symantec.com/>
- www.cert.org/nav/index_red.html
- <http://vil.nai.com/vil/>

Recent virus examples

➤ **W32/Netsky-P**

- ❑ Primarily spread through email
- ❑ Copies itself to various directories and shared folders
- ❑ Attempts to copy itself to C:\WINDOWS\FVProtect.exe. The name would make many people think this program was actually part of some antivirus utility.
- ❑ It also copies itself to C:\WINDOWS\userconfig9x.dll. Again, it would appear to be a system file, thus making people less likely to delete it.

Recent virus examples

➤ **Troj/Invo-Zip**

- ❑ A zip file attached to an email
- ❑ Email claimed zip file contains data related to an invoice, tax issue, or similar urgent paperwork
- ❑ Business people
- ❑ Steal financial data

➤ **MacDefender**

- ❑ Embedded in some web pages and when a user visits those web pages, he or she is given a fake virus scan that tells the user that they have a virus and it needs to be fixed. The “fix” is actually downloading a virus.
- ❑ Macintosh Computers

Recent virus examples

➤ **The Sobig Virus**

- ❑ It would copy itself to any shared drives on your network and it would email itself out to everyone in your address book

➤ **Mimail Virus**

- ❑ This virus not only collected email addresses from your address book, but also from other documents on your machine
- ❑ If you had a Word document on your hard drive and an email address was in that document
- ❑ Built in email engine

Recent virus examples

➤ **The Bagle Virus**

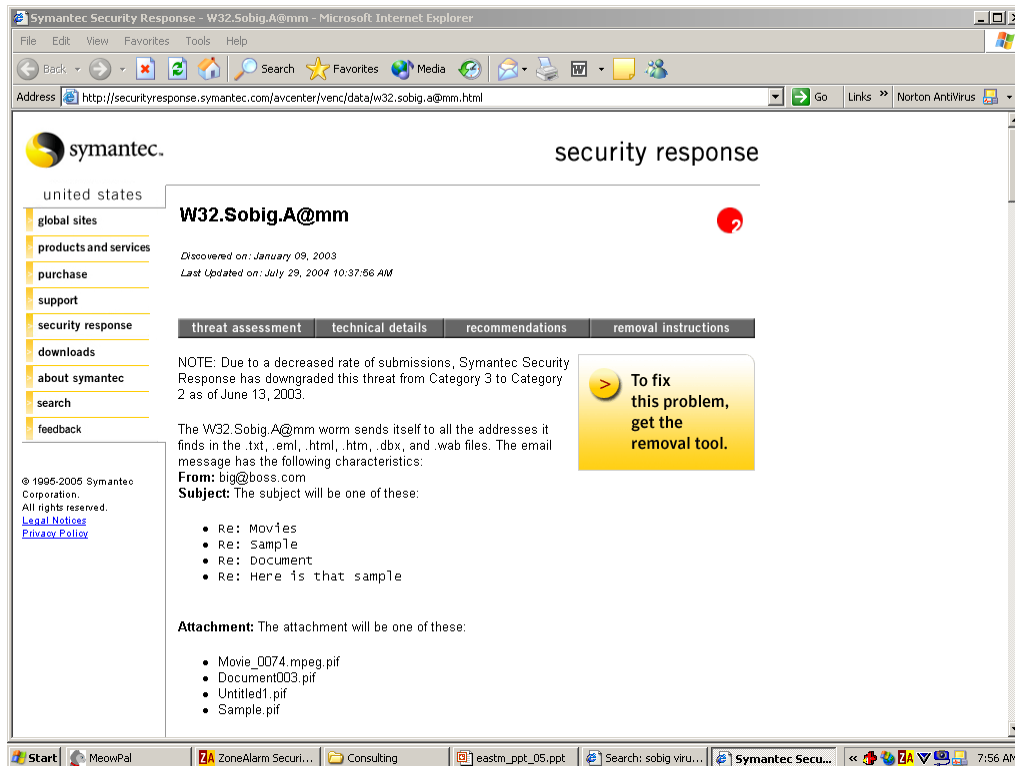
- The email it sent claimed to be from your system administrator. It would tell you that your email account had been infected by a virus and that you should open the attached file to get instructions
- This virus was particularly interesting for several reasons. To begin with, it spread both through email and copying itself to shared folders. Second, it could also scan files on your PC looking for email addresses. Finally, it would disable processes used by antivirus scanners

Recent virus examples

➤ **A Nonvirus Virus**

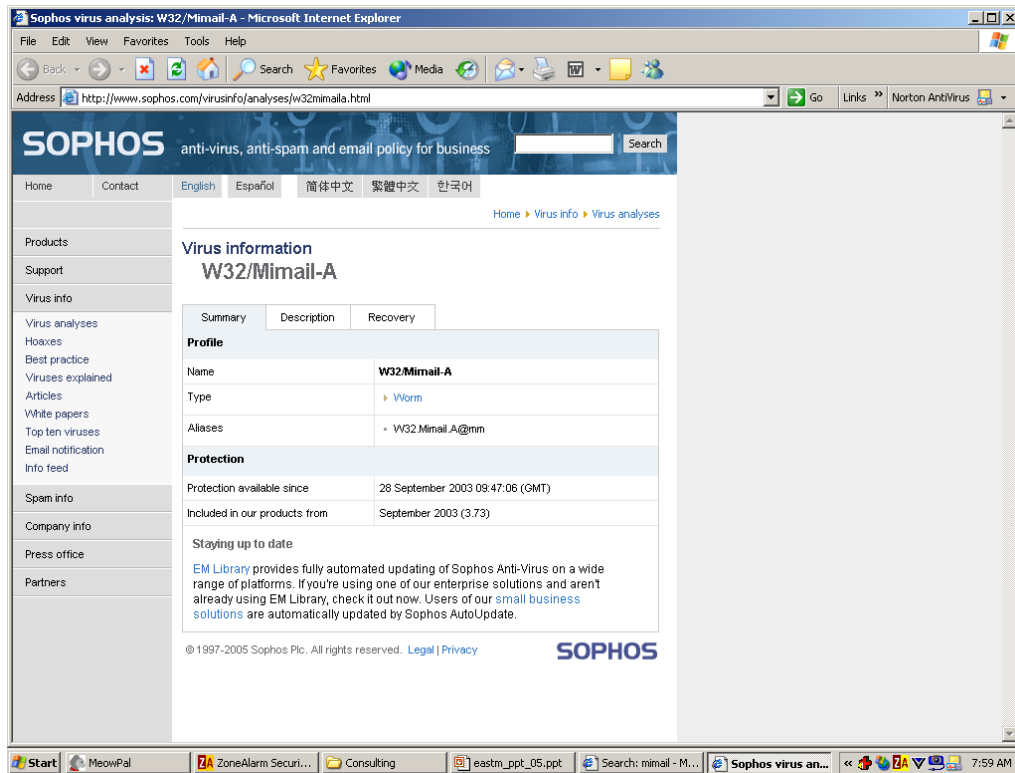
- ❑ A hacker sends an email to every address he has. The email claims to be from some well-known antivirus center and warns of a new virus that is circulating. The email instructs people to delete some file from their computer to get rid of the virus.

Viruses (cont.)



Symantic site information on the Sobig virus

Viruses (cont.)



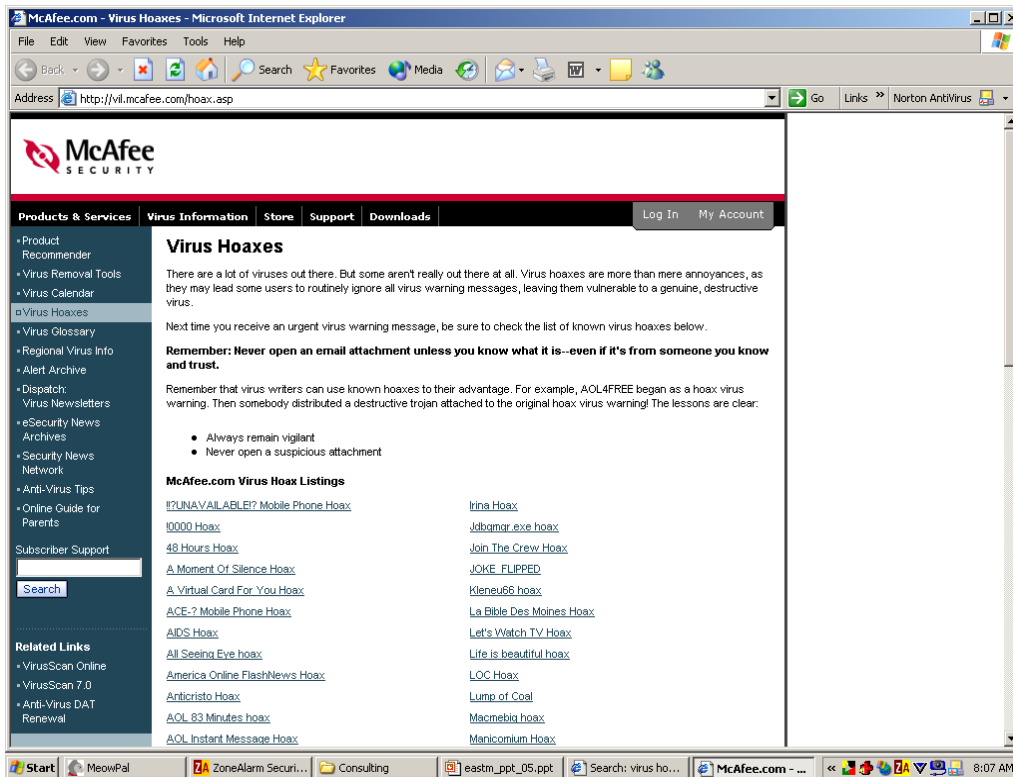
Information on the Minmail virus from the Sophos site

Viruses (cont.)



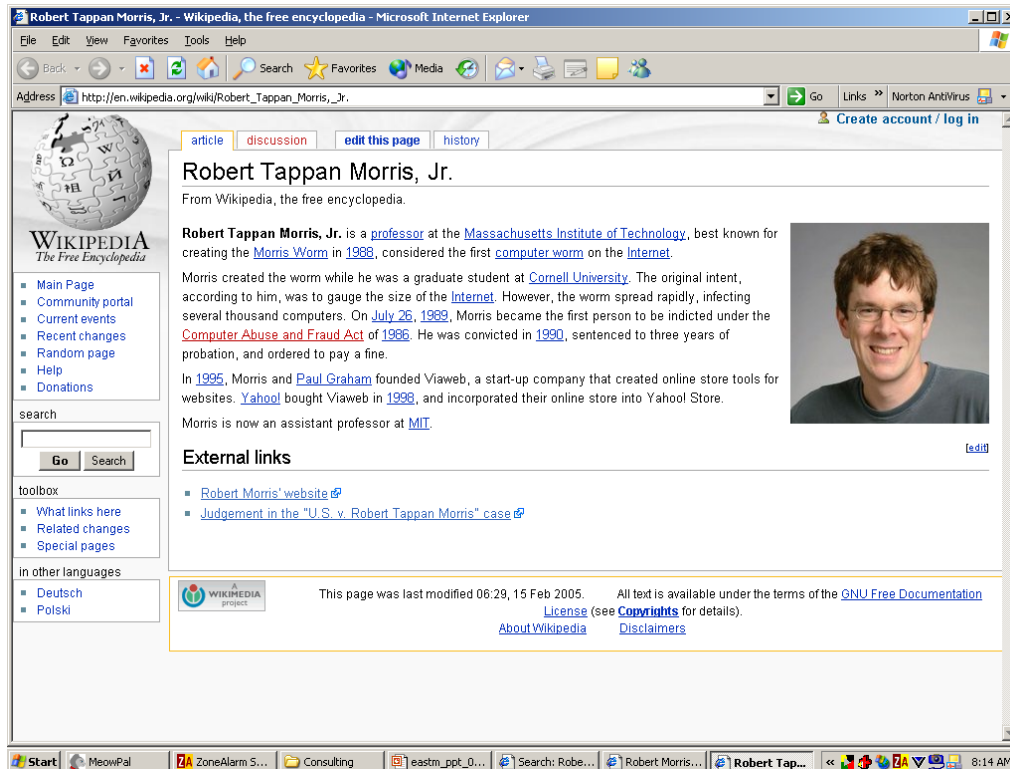
Information on the Bagle virus from the internet.com site

Viruses (cont.)



Virus hoaxes from the McAfee site

Viruses (cont.)



Wikipedia information on Robert Tappan Morris, Jr.

Viruses (cont.)

- Rules for avoiding viruses:
 - Use a virus scanner.
 - DO NOT open questionable attachments.
 - Use a code word for safe attachments from friends.
 - Do not believe “Security Alerts.”
 - Do not believe on email alert

Trojan Horses

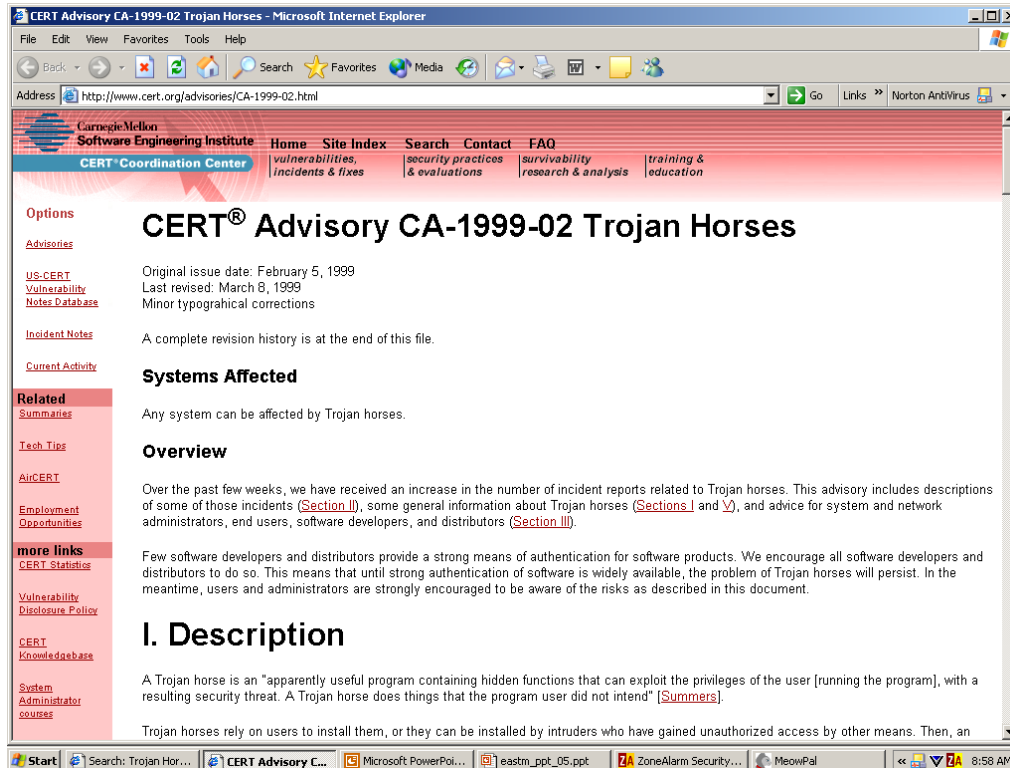
A program that looks benign, but is not

- A cute screen saver or apparently useful login box can
 - Download harmful software.
 - Install a key logger .
 - Open a back door for hackers.

Trojan Horses (cont.)

- Competent programmers can craft a Trojan horse:
 - To appeal to a certain person
- Company policy should prohibit unauthorized downloads.

Trojan Horses (cont.)

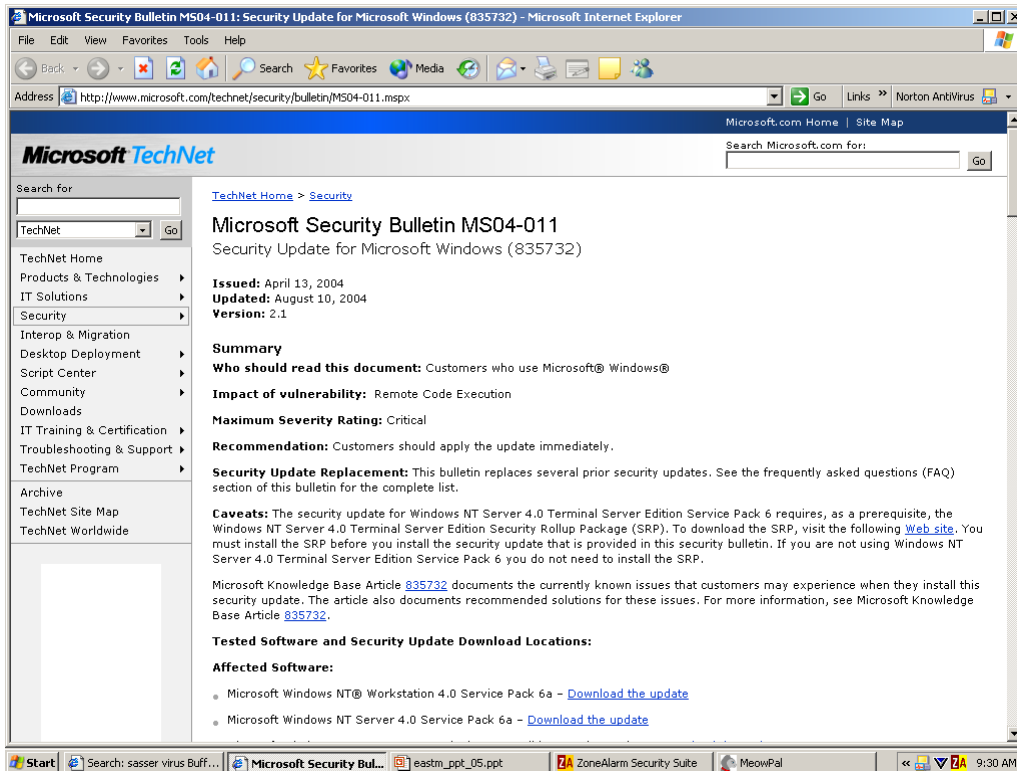


Still-valid CERT advisory on Trojan horses

The Buffer Overflow Attack

- Program writes data beyond the allocated end of a buffer.

The Buffer Overflow Attack (cont.)



A Microsoft Security Bulletin on a buffer overflow attack

The Buffer Overflow Attack (cont.)

The screenshot shows a Microsoft Internet Explorer browser window displaying the SecuriTeam website. The address bar shows the URL: <http://www.securiteam.com/securityreviews/5OP08006UQ.html>. The page title is "Writing Buffer Overflow Exploits - a Tutorial for Beginners". The article is dated "10 Apr. 2002". The page layout includes a sidebar on the left with links like "SecuriTeam Home", "Ask the Team", "Mailing Lists", and "Advertising Info". The main content area has a "Summary" section, a "Credit" section, and a "Details" section. The "Details" section is titled "1. Memory" and discusses the organization of memory in a process. The right sidebar contains a "Search" box and a "Related Articles" list. The bottom of the browser window shows the Windows taskbar with various icons and the system clock.

SecuriTeam.com™ - Writing Buffer Overflow Exploits - a Tutorial for Beginners - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://www.securiteam.com/securityreviews/5OP08006UQ.html> Go Links Norton AntiVirus

Free / Accurate / Independent

SecuriTeam
Beyond Security

SecuriTeam Home
Ask the Team
Mailing Lists
Advertising Info

SecuriTeam in Your Inbox

E-mail this article to a friend

New vulnerability? New tool? Tell us

RSS

Assembly Language
Step-by-step Tutorial and Reference Intel 8086 Microprocessor Emulator

"Smart" Threat Assessment
Computerized to determine risk. Practical solutions - Call Today!

Network Vulnerabilities
Find and eliminate them across the entire enterprise. Get info here!

Identify Network Risks
Free IM & P2P vulnerabilities assessment provides detailed report

Ads by Goooooogle

Security News - Security Reviews - Exploits - Tools - UNIX Focus - Windows Focus

Writing Buffer Overflow Exploits - a Tutorial for Beginners 10 Apr. 2002

Search
All Sections
Search

Summary

Buffer overflows in user input dependent buffers have become one of the biggest security hazards on the internet and to modern computing in general. This is because such an error can easily be made at programming level, and while invisible for the user who does not understand or cannot acquire the source code, many of those errors are easy to exploit. This paper attempts to teach the novice - average C programmer how an overflow condition can be proven to be exploitable.

Credit:
The information has been provided by Mixter.

Details

1. Memory

Note: The way we describe it here, memory for a process is organized on most computers, however it depends on the type of processor architecture. This example is for x86 and roughly applies to Sparc.

The principle of exploiting a buffer overflow is to overwrite parts of memory that are not supposed to be overwritten by arbitrary input and making the process execute this code. To see how and where an overflow takes place, let us look at how memory is organized. A page is a part of memory that uses its own relative addressing, meaning the kernel allocates initial memory for the process, which it can then access without having to know where the memory is physically located in RAM. The processes memory consists of three sections:

- Code segment, data in this segment are assembler instructions that the processor executes. The code execution is non-linear, it can skip code, jump, and call functions on certain conditions. Therefore, we have a pointer called EIP, or instruction pointer. The address where EIP points to always contains the code that will be executed next.

Related Articles

- Anti Brute Force Resource Metering
- Antidebugging For (M)asses - Protecting the Environment
- Removing about:blank Homepage Hijacker
- Remote Windows Kernel Exploitation - Step Into the Ring 0
- Blind Injection in MySQL Databases (via BENCHMARK)
- The Misuse of RC4 in Microsoft Word and Excel
- Hold Your Sessions: An Attack on Java Session-Id Generation
- Advanced SQL Injection in Oracle Databases
- Security Considerations for Web-based Applications
- The 30/20 Rule for Web Application Security
- Exploring Adjacent Memory Against stmpcpy
- Data Tastes Better Seasoned: Introducing the ASH Family of Hashing Algorithms
- SQL Injection Attacks by Example
- Hacking Bluetooth Enabled

Start Search: Buffer over... SecuriTeam.com eastn_ppt_05.ppt ZoneAlarm Security... MeowPal Solitaire 9:19 AM

Web tutorial for writing buffer overflows

Spyware

- Requires more technical knowledge
- Usually used for targets of choice

Spyware (cont.)

- Forms of spyware
 - Web cookies
 - Key loggers

Spyware (cont.)

- Legal Uses

- Monitoring children's computer use
- Monitoring employees

- Illegal Uses

- Deployment will be covert

Spyware (cont.)

SpywareRemoversReview
Side-by-side Comparisons of Top Spyware Removers

Current Reviews: 5
Updated: March 24, 2005

Spyware Removers 2005 - Overview

Overview
Spyware and Adware viruses have rapidly become the number one threat to your computer with over 90% of computers already infected. These include "Trojans", Web Bugs, Advertiser Software, Monitoring Software and more. Fortunately there are good Spyware and Adware virus removal tools available. Sorting through them all to find the right one is a challenging task and an important decision to make. We've gone through dozens and come up with a short list of the best.

Background - What is Spyware, Adware and Malware?
Spyware and Adware, also called "Malware", are files made by publishers that allow them to snoop on your browsing activity, see what you purchase and send you "pop-up" ads. They can slow down your PC, cause it to crash, record your credit card numbers and worse. If you're like most Internet users, chances are you're probably infected with these files. Simply surfing the Internet, reading email, downloading music or other files can infect your PC without you knowing it.

Our Testing Results
In our random PC testing, every single one has been infected with Spyware and Adware - some with dozens of infections - even those PCs consistently using well-known Virus and Firewall software. They are now Spyware and Adware free!

Bottom Line - What's the Best Way to Eliminate Spyware, Adware and Malware?
Use a good Spyware/Adware/Malware remover such as the ones presented below. Using one that is at least moderately popular is a good idea because it has been tested and used by many users. Each of the sites selected here fall into that category, although [XoftSpy](#) and [NoAdware](#) are the most popular. XoftSpy detects the widest variety of threats, while NoAdware is the easiest to use. XoftSpy has a very high satisfaction rate and gets the slight nod as our top choice.

#	Site (click screenshot to visit)	FREE Scan	Site Comments	Popularity/ Satisfaction	Ease of Use	Additional Comments	Current Rating	Site Link
1.		✓	Straightforward, easy to read site. Detects the widest variety of spyware, adware and other threats we've seen. Provides free updates.	High / Very High	Easy	Our top choice. XoftSpy has grown rapidly popular. Very easy to use and thorough. Finds, categorizes and assesses threats for free.	9.8 / 10 Best	Go

Example of free spyware removal software

How Is Spyware Delivered to a Target System?

- Website
- Trojan Horse
- An employer (or parent) is installing the spyware, it can then be installed non-covertly

Other Forms of Malware

- Rootkit
 - A collection of hacking tools that can
 - Monitor traffic and keystrokes
 - Create a backdoor
 - Alter log files and existing tools to avoid detection
 - Attack other machines on the network

Malicious Web-Based Code

- Web-Based mobile code
 - Code that is portable on all operating systems
 - Spreads quickly on the web

Logic Bombs



Spam



Detecting and Eliminating Viruses and Spyware

- Antivirus software operates in two ways:
 - Scans for virus signatures
 - Keeps the signature file updated
 - Watches the behavior of executables
 - Attempts to access e-mail address book
 - Attempts to change Registry settings
 - Attempting to copy itself



Detecting and Eliminating Viruses and Spyware (cont.)

■ Anti-spyware software

- ❑ www.webroot.com
- ❑ www.spykiller.com
- ❑ www.zerospy.com
- ❑ www.spectorsoft.com



Summary

- There are a wide variety of attacks.
- Computer security is essential to the protection of personal information and your company's intellectual property.
- Most attacks are preventable.
- Defend against attacks with sound practices plus antivirus and antispyware software.