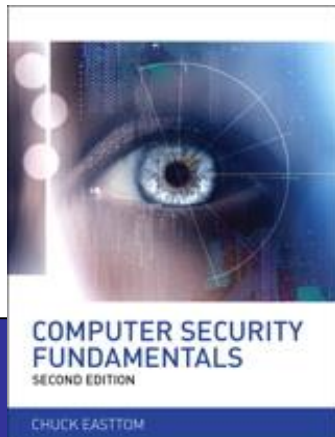


Computer Security Fundamentals

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

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



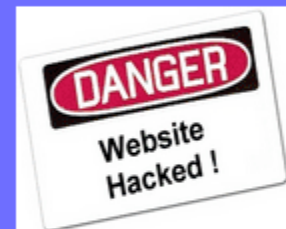
Suspicious
popup ads



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**

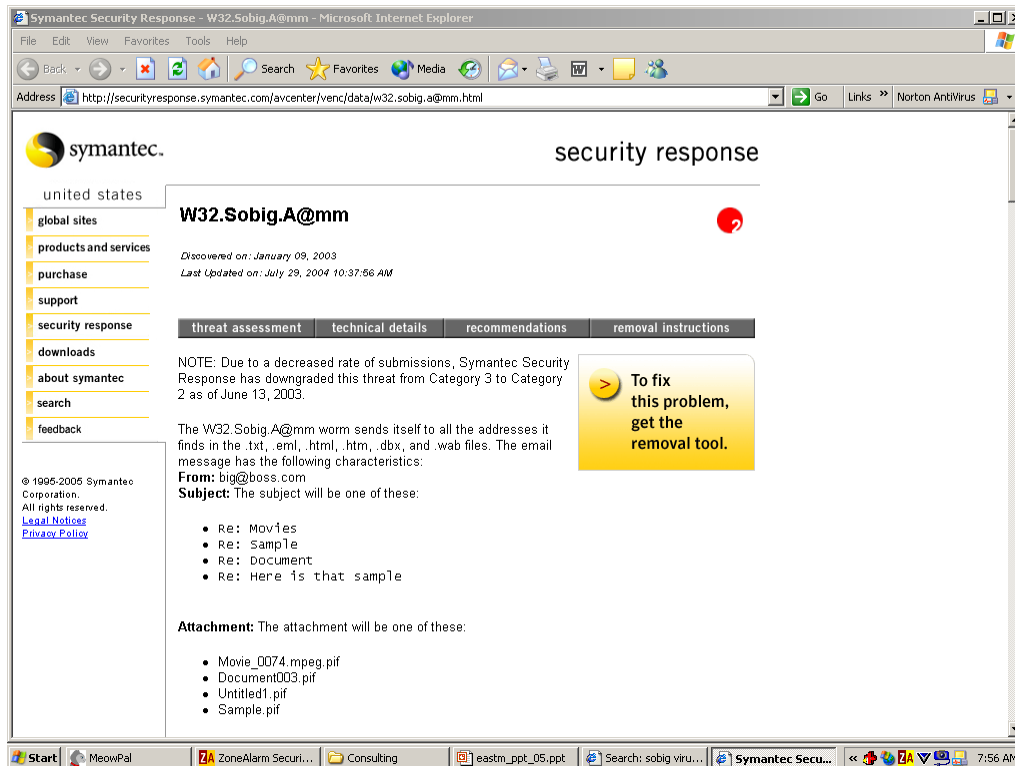
- The email it sent claimed to be from your system administrator. It would tell you that your email account had been infected by a virus and that you should open the attached file to get instructions
- This virus was particularly interesting for several reasons. To begin with, it spread both through 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**

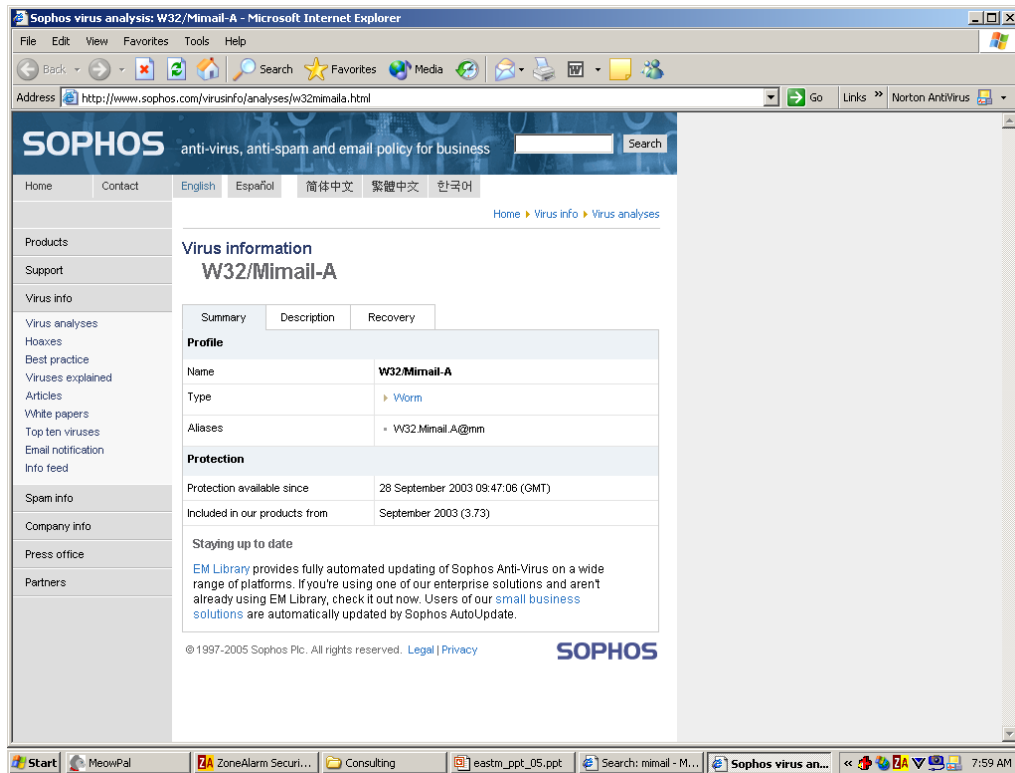
- ❑ A hacker sends an email to every address he has. The email claims to be from some well-known antivirus center and warns of a new virus that is circulating. The email instructs people to delete some file from their computer to get rid of the virus.

Viruses (cont.)



Symantic site information on the Sobig virus

Viruses (cont.)



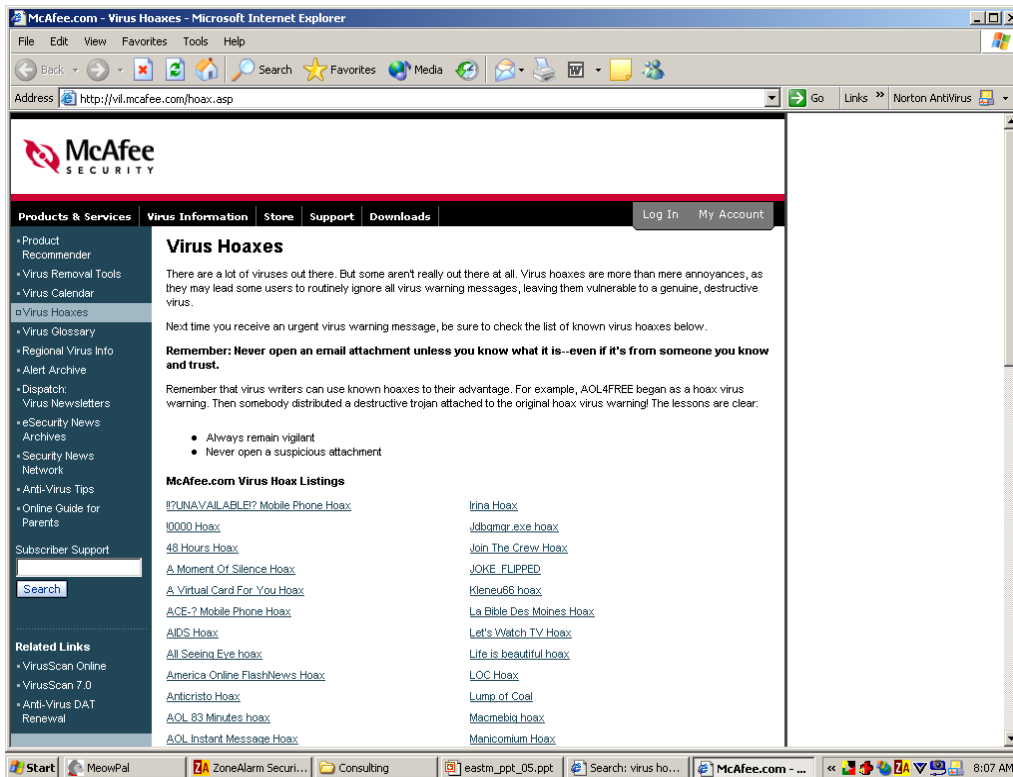
Information on the Minmail virus from the Sophos site

Viruses (cont.)



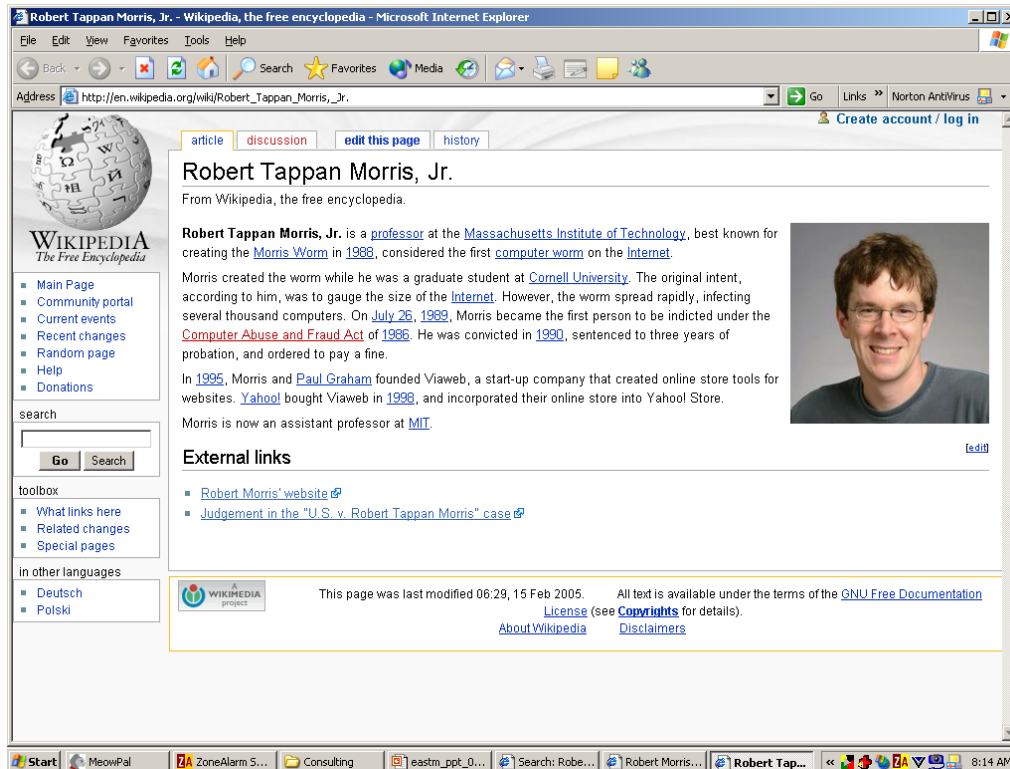
Information on the Bagle virus from the internet.com site

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

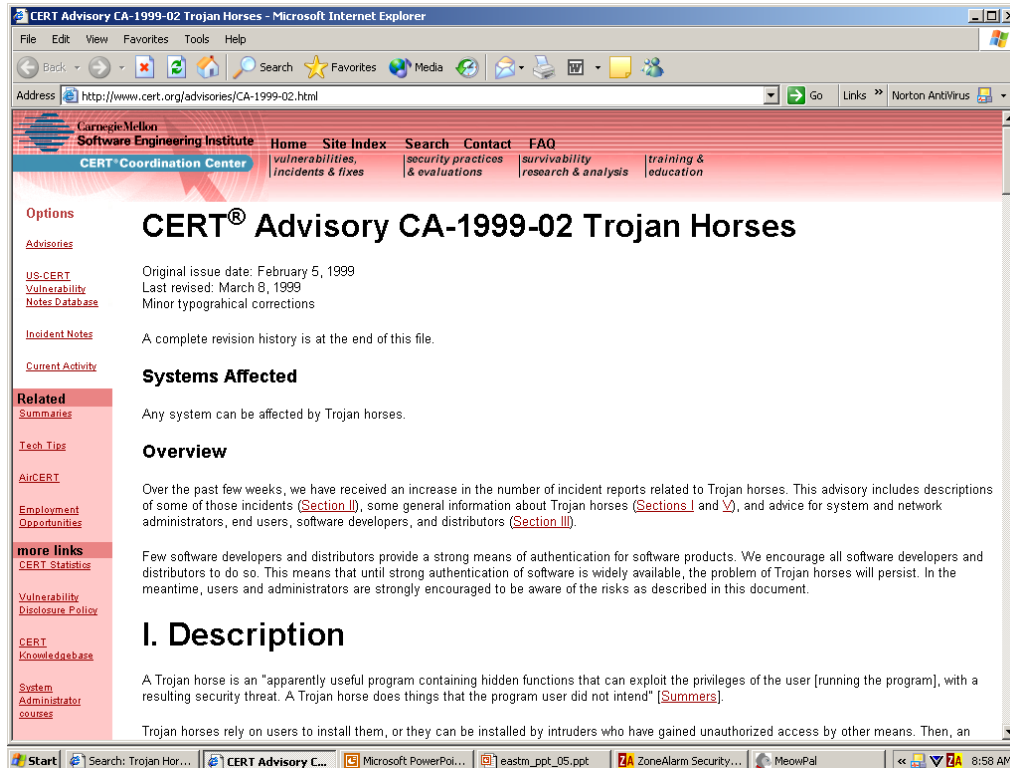
A program that looks benign, but is not

- 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.)

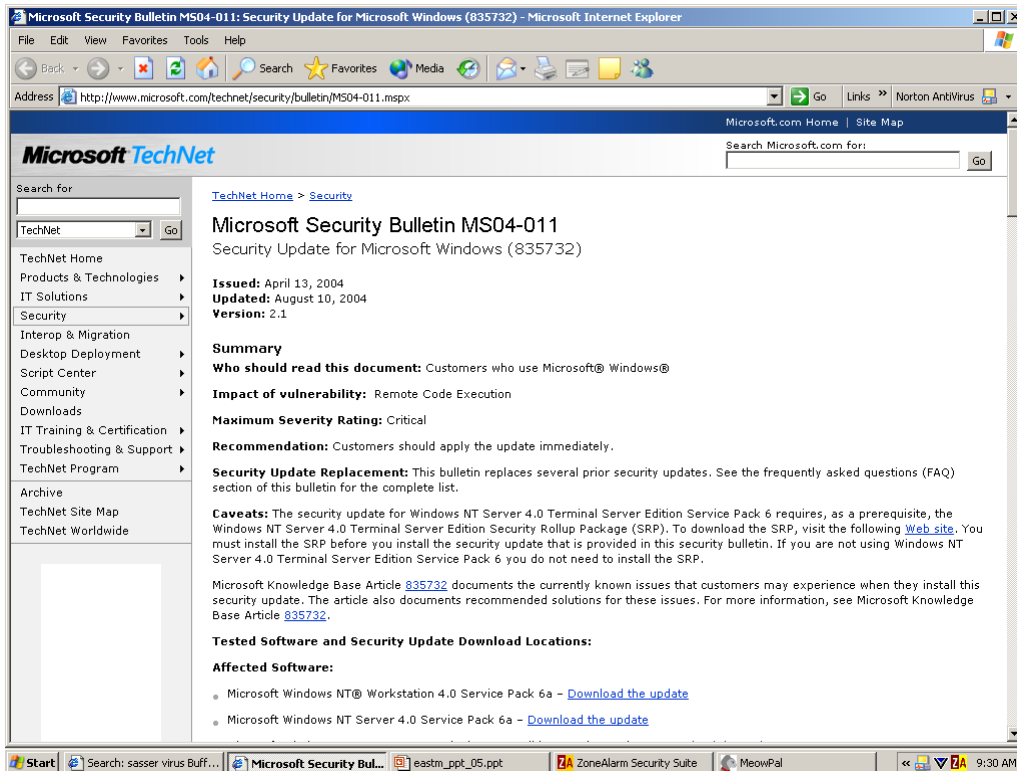


Still-valid CERT advisory on Trojan horses

The Buffer Overflow Attack

- Program writes data beyond the allocated end of a buffer.
- Valid data can be overwritten.
- Can cause execution of arbitrary (and potentially malicious) code.

The Buffer Overflow Attack (cont.)



A Microsoft Security Bulletin on a buffer overflow attack

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.)

Compare Top Spyware Removers - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://www.spywareremoversreview.com/>

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.

Comparisons of Top Spyware Removers

#	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

Start Search: spyware - Micro... Compare Top Spywar... eastm_ppt_05.ppt ZoneAlarm Security Suite MeowPal 9:43 AM

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.