Streettech Antivirus Seminar

Tues, Thurs, Aug. 12, 14
Conducted by Lenny Bailes

Lecture Notes

AV Links

Computer Virus Myths and Hoaxes http://www.vmyths.com/fas/fas1.cfm

Computer Virus FAQ for New Users http://www.faqs.org/faqs/computer-virus/new-users/

Virus Encyclopedia http://www3.ca.com/virusinfo/browse.

Step-By-Step: Set Antivirus Software for Maximum Protection
http://www.pcworld.com/howto/article/0,aid,106718,pg,1,00.asp

Cornell Seminar Digital Immunity http://www.cit.cornell.edu/security/virus/lecture-june02/immunity/

Lenny's AV FAQ http://www.techweb.com/winmag/library/1998/0101/featu101.htm
Topics to discuss in Streettech AV Seminar:

Net Security Quiz http://netsecurity.about.com/library/blcomsec101-9.htm

Day 1 (3 hrs)

Why should I care about computer viruses?

1. What is a computer virus?

A computer virus is a program designed to spread itself by first infecting executable files or the system areas of hard and floppy disks and then making copies of itself. Viruses usually operate without the knowledge or desire of the computer user.

2. What kind of files can spread viruses?

Viruses have the potential to infect any type of executable code, not just the files that are commonly called 'program files'. For example, some viruses infect executable code in the boot sector of floppy disks or in system areas of hard drives. Another type of virus, known as a 'macro' virus, can infect word processing and spreadsheet documents that use macros. And it's possible for HTML documents containing JavaScript or other types of executable code to spread viruses or other malicious code.

Since virus code must be executed to have any effect, files that the computer treats as pure data are usually not infecton vectors. These includes graphics and sound files such as .gif, .jpg, .mp3, .wav, etc., as well as plain text in .txt files. Just viewing picture files won't infect your computer with a virus. The virus code usually has to be in a form, such as an .exe program file , a Word .doc file, or a Windows script (VBA, Java, Javascript) that the computer will actually try to execute
.
However, sounds and graphics embedded with hostile script instructions can be used to create hardware annoyances, or compromise computer security,

What kind of files can spread viruses?
a) boot sector (floppy disks)
b) executable files (.COM or .EXE extension)
c) polymorphic (virus mutates the code it writes to new files, making it harder to detect)
d) multipartite (viruses that combine boot sector and file-writing with other means of infection)
d) email (Word and Excel macro viruses)
e) scripts (Visual Basic and Hostile Java/Javascript/Asp)

3. How do viruses affect computer performance?

Viruses are software programs, and they can do the same things as any other programs running on a computer. The actual effect of any particular virus depends on how it was programmed by the person who wrote the virus.

Some viruses are deliberately designed to damage files or otherwise interfere with your computer's operation, while others don't do anything but try to spread themselves around. But even the ones that just spread themselves are harmful, since they damage files and may cause other problems in the process of spreading.

Note that viruses can't usually do damage to hardware: they won't melt down your CPU, burn out your hard drive, cause your monitor to explode, etc. Warnings about viruses that will physically destroy your computer are usually hoaxes, not legitimate virus warnings. (Updated note: it is possible to cause damage to a computer monitor in some operating systems by switching the screen resolution to an unsupported scan rate. This is harder to do in Windows than in Linux.)

How viruses affect computer performance -- warning symptoms:

- Hard disk thrashing
- Unusually sluggish performance (exaggerated time to boot into GUI, save or open file)
- Odd program behavior (files refusing to save, strange popup messages, deterioration of screen display, protection faults and program crashes)
- New, unexpected error messages during boot process,

4. How do viruses spread?

When you execute program code that's infected by a virus, the virus code will also run and try to infect other programs, either on the same computer or on other computers connected to it over a network . And the newly infected programs will try to infect yet more programs.

When you share a copy of an infected file with other computer users, running the file may also infect their computers; and files from those computers may spread the infection to yet more computers.

If your computer is infected with a boot sector virus, the virus tries to write copies of itself to the system areas of floppy disks and hard disks. Then the infected floppy disks may infect other computers that boot from them, and the virus copy on the hard disk will try to infect still more floppies.

Some viruses, known as 'multipartite' viruses, can spread both by infecting files and by infecting the boot areas of floppy disks.

5. What kinds of Malware can infect your computer? (Bombs, Trojans, Hoaxes)

Malware can infect

Program files
Files that contain executable portions, such as macros
Diskettes and other storage media
Email message attachments

HTML based email messages

Malware cannot infect

Hardware (though it can be malicious)
Text based files or messages
Write-protected storage media

Slide 009 definition of malware
Slide 010 definition of Worm
Slide 011 example of Worm
Slide 012 definition of Trojan
Slide 013 example of Trojan
Slide 014 definition of Joke
Slide 015 example of Joke
Slide 016 definition of Hoax
Slide 017 example of Hoax
Slide 018 definition of Logic Bomb
Slide 019 example of Logic Bomb (sometimes logic bombs trigger a real virus)
Slide 020 definition of Internet Threat (class see http://www.gondek.org/rich/hjavaex.htm)

A type of program that is often confused with viruses is a 'Trojan horse' program. This is not a virus, but simply a program (often harmful) that pretends to be something else.

For example, you might download what you think is a new game; but when you run it, it deletes files on your hard drive. Or the third time you start the game, the program E-mails your saved passwords to another person.

Note: simply downloading a file to your computer won't activate a virus or Trojan horse; you have to execute the code in the file to trigger it. This could mean running a program file, or opening a Word/Excel document in a program (such as Word or Excel) that can execute any macros in the document.

6. **How do antivirus utilities protect your computer (and network) from infection**
   a) free online scanning from Trend (http://kb.trendmicro.com/solutions/default.asp)
   b) demonstrate Norton AV (scanning and realtime protection) c) demonstrate network deployment of Corporate Norton AV ((Randal may want to do this))

For NAV Tutorials, see http://itexpress.ucdavis.edu/help/tutorials/NAVPC.shtml
http://www.symantec.com/techsupp/nav/nav2001_info_tutorial.html
http://www.symantec.com/techsupp/nav/nav_2002_info_tutorial.html

5. How does a computer become exposed to viruses?

The most common traditional way for viruses to spread until around 2000 was through promiscuous use of floppy diskettes. Other vectors of infection include shared files on servers, websites containing hostile code, corrupted shareware or pirate programs on hacker bulletin boards, transmission through scripts in e-mail attachments, and unsecured computers in LAN and WAN environments.

6. What's the story on viruses and E-mail?

You can't get a virus just by reading a plain-text E-mail message or Usenet post. What you have to watch out for are encoded messages containing embedded executable code (i.e., JavaScript in

an HTML message) or messages that include an executable file attachment (i.e., an encoded program file or a Word document containing macros).

In order to activate a virus or Trojan horse program, your computer has to execute some type of code. This could be a program attached to an E-mail, a Word document you downloaded from the Internet, or something received on a floppy disk. There's no special hazard in files attached to Usenet posts or E-mail messages: they're no more dangerous than any other file.

Day 2 (3hrs)

1. How do e-mail viruses work and spread?
   a) Anatomy of Microsoft Word and Excel viruses
   b) Other Visual Basic viruses
2. What are the limitations of AV programs and firewalls? (Measures can you take to remove viruses that slip past your AV program.)
3. Which common system settings can you monitor and modify to provide additional protection

7. What can I do to reduce the chance of getting viruses from E-mail?

8. The limitations of firewalls and anti virus

Treat any file attachments that might contain executable code as carefully as you would any other new files: save the attachment to disk and then check it with an up-to-date virus scanner before opening the file.

If your E-mail or news software has the ability to automatically execute JavaScript, Word macros, or other executable code contained in or attached to a message, I strongly recommend that you disable this feature. My personal feeling is that if an executable file shows up unexpectedly attached to an E-mail, you should delete it unless you can positively verify what it is, who it came from, and why it was sent to you.=

The outbreak of the Melissa and Loveletter viruses were a vivid demonstration of the need to be extremely careful when you receive E-mail with attached files or documents. Just because an E-mail appears to come from someone you trust, this does NOT mean the file is safe or that the supposed sender had anything to do with it.

Some general tips on avoiding virus infections:

1. Install anti-virus software from a well-known, reputable company, UPDATE it regularly, and USE it regularly.

New viruses come out every single day; an a-v program that hasn't been updated for several months will not provide much protection against current viruses.

2. In addition to scanning for viruses on a regular basis, install an 'on access' scanner (included in most good a-v software packages) and configure it to start automatically each time you boot your system. This will protect your system by checking for viruses each time your computer accesses an executable file.

3. Virus scan any new programs or other files that may contain executable code before you run or open them, no matter where they come from. There have been cases of commercially distributed floppy disks and CD-ROMs

spreading virus infections.

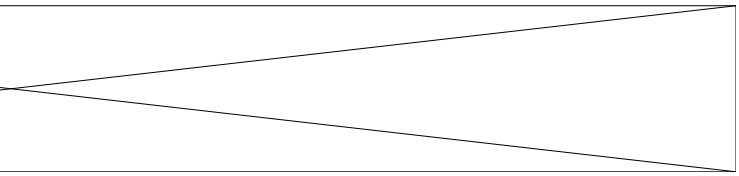
4. Anti-virus programs aren't very good at detecting Trojan horse programs, so be extremely careful about opening binary files and Word/Excel documents from unknown or 'dubious' sources. This includes posts in binary newsgroups, downloads from web/ftp sites that aren't well-known or don't have a good reputation, and executable files unexpectedly received as attachments to E-mail or during an on-line chat session.

5. If your E-mail or news software has the ability to automatically execute JavaScript, Word macros, or other executable code contained in or attached to a message, I strongly recommend that you disable this feature.

6. Be _extremely_ careful about accepting programs or other files during on-line chat sessions: this seems to be one of the more common means that people wind up with virus or Trojan horse problems. And if any other family members (especially younger ones) use the computer, make sure they know not to accept any files while using chat.

7. Do regular backups. Some viruses and Trojan horse programs will erase or corrupt files on your hard drive, and a recent backup may be the only way to recover your data.

Ideally, you should back up your entire system on a regular basis. If this isn't practical, at least backup files that you can't afford to lose or that would be difficult to replace: documents, bookmark files, address books, important E-mail, etc.



F-Secure Virus Descriptions

Alphabetical Index

Select from the list Go

Select from the list Go

NAME: **Junkie**
ALIAS: Malmo
ORIGIN: Sweden
SIZE: 1035
TYPE: Resident Boot sectors MBR COM-files
REPAIR: Yes

The Junkie virus was circulated through European BBSs at the end of May 1994. It travelled in a file called HV-PSPTC.ZIP. According to the description, the file was supposed to contain a program which would make it possible to install illegal copies of the Pacific Strike-game directly from the hard disk instead of from diskettes. The packet's content, PSPATCH.COM, contained only the Junkie virus, however.

Junkie is a Swedish multipartite virus. It infects hard disk MBRs and COM files. When an infected file is executed in a computer for the first time, the virus overwrites the hard disk's MBR with its own code but does nothing else. During its next execution, the virus goes resident in memory and infects all accessed COM files. Junkie is a fast infector.

Junkie also infects boot sectors of all floppies used in the machine, and is capable of spreading further when the machine is booted up from such a diskette. 360KB and 2.88MB diskettes are not infected.

Infected COM files grow by approximately 1035 bytes. Since the virus infects all accessed COM files, it corrupts files which are structurally EXEs but happen to have the extension COM. The virus code is doubly encrypted. The following message is hidden under the second encryption layer:

Dr White - Sweden 1994
Junkie Virus - Written in Malmo...M01D

Dr White has also written another Swedish virus called Desperado.
The Junkie virus can be noticed by the decrease of available memory in the system. Some programs also display the message "Program too big to fit in memory" when they are executed.
TECHNICAL INFO: Junkie patches floppy boot sectors and HD MBS from offset 98 to 127. The virus code itself is contained in two sectors, 0,0,4-5 on HD and on the last track (40 or 80), side 1, sectors 8-9 on floppies. Junkie does not relocate nor store the original sector anywhere. In COM files, the virus will append itself at the end of the file, with a length of 1027 to 1042 bytes.
Junkie is a selective fast infector (not all files will be infected on opening, just some). Junkie will not infect COM files shorter than about 5000 bytes. However, Junkie will sometimes infect files with other extensions, such as CO_, COW etc.
When active, Junkie will decrease the base memory by three kilos. Also, INT 1Ch will be hooked and QEMM will complain about and will not load high programs requiring this handler.
F-Secure anti-virus products are able to detect and disinfect the Junkie virus in both files and boot sectors.
[Analysis: Mikko Hypponen, F-Secure]

Security & Privacy

Security & Privacy Home

What You Should Know About the Blaster Worm

August 12, 2003

At 11:34 A.M. Pacific Time today, Microsoft began investigating a worm reported by Microsoft Product Support Services (PSS).

Related Resources

- Get More Details in the Technical Virus Alert

Glossary Terms

Click the term to get the definition from our Security and Privacy Glossary.

- virus
- worm

Why We Are Issuing This Alert

A new worm known as W32.Blaster.Worm (also known as MBlaster, W32/Lovsan.worm, MSBlast, W32.blaster.worm, Win32.posa.worm, Win32.poza.worm) has been identified that is seeking to exploit the vulnerability patched with Microsoft Security Bulletin MS03-026. Blaster is designed to launch a denial of service attack against Microsoft's Windows Update Web site.

Products Affected

The following products are affected:

- Microsoft® Windows NT® 4.0
- Microsoft Windows® 2000
- Microsoft Windows XP
- Microsoft Windows Server™ 2003

Prevention

If you are using Windows NT 4.0, Windows 2000, Windows XP, or Windows Server 2003, you should follow these steps to help protect your system:

1. Make sure you have a firewall.
    - If you have Windows XP or Windows Server 2003, enable the Internet Connection Firewall (ICF).
    - If you have Windows 2000 or Windows NT, visit Windows Catalog for a list of Internet firewall software.

2. Get the latest critical updates for the version of Windows that you are using and make sure you get the update addressed in Security Bulletin MS03-026.

3. Make sure you install and use antivirus software.

    - If you have antivirus software installed, get the latest virus definitions from your antivirus vendor's Web site.

    - If you do not have antivirus software installed, visit Windows Catalog for a list of antivirus software vendors.

What to Do If You Think Your Computer Has Been Infected

If you think your computer has been infected with the Blaster worm, please contact Microsoft Product Support Services or your antivirus vendor for assistance removing it.

- For Microsoft Product Support Services within the United States and Canada, call toll-free (866) PCSAFETY (727-2338).

- For Microsoft Product Support Services outside the United States and Canada, visit the Product Support Services Web page.

Additional Resources

- Get more technical details about Microsoft Security Bulletin MS03-026

- Get more info on protecting your computer from viruses