

Worms, Viruses, Trojans

And other malicious code

Brent Selch

Appriss, Inc.

Overview

- Viruses
- Trojans
- Worms
- Spyware

What is a Virus?

- To be defined as a virus, a program must:
 - Replicate
 - Be dependent on a "host"
 - Create damage to the infected system

Simple Definition

- A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. Thus, a computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells.

Simple Definition

- A virus is a program which
 - Reproduces itself
 - Hides in other computer code without permission
 - Does nasty or undesirable things not intended by its victim

Virus Effects

- Trivial
 - Simply reproduces or displays messages
- Minor
 - Alters or deletes files

Virus Effects

- Moderate
 - Wipes out entire disk drive contents
- Major
 - Slowly corrupts data with pattern, making restoration difficult

Virus Effects

- Severe
 - Slowly corrupts data without pattern, making restoration impossible.

Virus Components

- The Replication Mechanism
 - To allow virus to copy itself
- The Protection Mechanism
 - Hides virus from detection

Virus Components

- The Trigger
 - Mechanism which will set off the payload
- The Payload
 - Effect of the virus

Virus Types

- Viruses classifications:
 - Boot Viruses
 - File Viruses
 - Multi-partite Viruses
 - Polymorphic Viruses
 - Meta Viruses

Boot Viruses

- Infect the boot block on a bootable device
- Usually replaces the boot block with all or part of a virus program
- Most have trigger dates
- Memory resident to infect other devices

Boot Virus Example

- Michaelangelo
 - On March 6 (Michaelangelo's birthday) garbage is written throughout the entire drive

File Viruses

- Infect executable files
- Usually append the virus code to the file
- Damage is done when executed

File Virus Example

- Friday the 13th
 - If the date matches Friday the 13th when the infected executable is run, all .EXE files are deleted.

Multi-Partite Viruses

- Infect both boot blocks and executable files
- Combine the capabilities of both boot and file viruses

MP Virus Example

- Tequila
 - Will display graphics and text rather than running the intended programs.

Polymorphic Viruses

- Can infect boot sector, executable files, or both
- Is self modifying, changing each time it infects
- Very difficult to detect and remove

Poly Virus Example

- Tremor
 - Triggers 3 months after infection and displays “-MOMENT-OF-TERROR-IS-THE-BEGINNING-OF-LIFE-” with every warm boot

Meta Viruses

- First viruses to infect data files and to work on multiple platforms
- Carried in data files such as Microsoft Word .doc format and AmiPro documents

Meta Virus Example

- Concept
 - Will infect the global template and all files loaded from then on.
 - Was distributed by Microsoft on a CD-ROM called Microsoft Windows 95 Software Compatibility Test

Virus Prevention

- Never use a “foreign” disk or CD without scanning it for viruses
- Always scan files downloaded from the internet or other sources
- Never boot your PC from a floppy unless you are certain that it is virus free
- Write protect your disks

Virus Prevention

- Use licensed software
- Password protect your PC to prevent unattended modification
- Make regular backups
- Install and use antivirus software
- Keep antivirus software up to date

Information on Viruses

- Symantec Security Response
 - <http://securityresponse.symantec.com/>
- McAfee Virus Information Library
 - <http://vil.mcafee.com/>
- Secunia Virus Information
 - http://secunia.com/virus_information/

Computer Trojans

- Malicious computer programs disguised as something useful
- The major difference between viruses and trojans
 - Viruses reproduce
 - Trojans are installed

Computer Trojans

- Most common way of virus introduction
- Example
 - Program called pkz300b.exe
 - Disguises itself as an archiving utility
 - When run it will delete the contents of your hard drive

Computer Worms

- Self-reproducing programs that run independantly
- Propagate via network connections

Worm Examples

- Slapper
 - Slapper is a network worm that spreads on Linux machines by using a flaw discovered in August 2002 in OpenSSL libraries. The worm was found in Eastern Europe late on Friday September 13th 2002

Worm Examples

- Fizzer
 - A complex e-mail worm that can spread itself in e-mails and in the Kazaa P2P (peer-to-peer) file-sharing network.

Worm Examples

- Fizzer (continued)
 - Contains a built-in IRC backdoor, a DoS attack tool, a keylogger, an HTTP server and other components.

Worm Examples

- Fizzer (continued)
 - Has the functionality to kill the tasks of certain anti-virus programs. Additionally, the worm has automatic updating capabilities.

Worm Examples

- SQL Snake
 - A worm that spreads among machines running Microsoft SQL Server using the default system administrator account ("sa") with an empty password to infect the system.

Spyware

- A broad category of malicious software intended to intercept or take partial control of a computer's operation without the user's informed consent.

Spyware

- While the term taken literally suggests software that surreptitiously monitors the user as a spy would, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

Spyware

- Spyware programs differ from computer viruses and worms in that they do not usually self-replicate. However, spyware also differs from earlier categories of malware in that it is almost always designed explicitly for commercial or financially fraudulent exploitation of the infected computer.

Spyware

- Within this generalization, however, spyware programs exhibit many different behaviors.

Spyware

- These include
 - unsolicited pop-up advertisements;
 - theft of personal financial information
 - monitoring of Web browsing activity for marketing purposes
 - re-routing of Web page requests to sites filled with ads profitable to the offender.

Spyware Removal

- To avoid spyware issues altogether, networked computer users should refrain from installing any piece of software that seems too good to be true, such as bogus "free" music downloads and the like.

Spyware Removal

- Advice for Windows users:
 - Keep up-to-date with patches using Windows Update
 - Keep antivirus software up-to-date
 - Disable Active-X, or use alternate browsers such as Mozilla Firefox or Opera

Spyware Removal

- Install anti-spyware software such as:
 - Microsoft AntiSpyware Beta: <http://www.microsoft.com/athome/security/spyware/software/default.mspix>
 - Lavasoft AdAware: <http://lavasoftusa.com>
 - SpyBot-Search & Destroy: <http://security.kolla.de>

References

- <http://en.wikipedia.org/wiki/Spyware>
- http://en.wikipedia.org/wiki/Computer_virus
- <http://vil.mcafee.com>
- http://secunia.org/virus_statistics/
- <http://www.microsoft.com/security/>

Questions

- Slides available at <http://xenowolf.com> after class