CS 465 Computer Security

Kent Seamons

Sources:
- Schneier, Secrets and Lies
- Stallings, Network Security Essentials
Attacks on Computers on the Internet

- Malicious software - malware
  - Viruses
  - Worms
  - Trojan horses

- Two components
  - Payload
  - Propagation mechanism
Computer Viruses

- A string of computer code that attaches itself to another program (it can’t live on its own)
- Three categories of viruses
  - File infectors
  - Boot sector viruses
  - Macro (interpreted) viruses
- Macro viruses are the future
- Polymorphic viruses mutate with every infection
Worms

- A piece of malware particular to networked computers
- Self-replicating program that does not hide in another program
- Propagates through the network
Trojan Horse

- Piece of malware embedded in some "normal" piece of software
Viruses and “Malicious Programs”

- Computer “Viruses” and related programs have the ability to replicate themselves on an ever increasing number of computers. They originally spread by people sharing floppy disks. Now they spread primarily over the Internet (a “Worm”).

- Other “Malicious Programs” may be installed by hand on a single machine. They may also be built into widely distributed commercial software packages. These are very hard to detect before the payload activates (Trojan Horses, Trap Doors, and Logic Bombs).
Taxonomy of Malicious Programs

Malicious Programs

Need Host Program
- Trapdoors
- Logic Bombs
- Trojan Horses
- Viruses

Independent
- Bacteria
- Worms

Replicate
Definitions

- **Virus** - code that copies itself into other programs.
- A “**Bacteria**” replicates until it fills all disk space, or CPU cycles.
- **Payload** - harmful things the malicious program does, after it has had time to spread.
- **Worm** - a program that replicates itself across the network (usually riding on email messages or attached documents (e.g., macro viruses).
Definitions

- **Trojan Horse** - instructions in an otherwise good program that cause bad things to happen (sending your data or password to an attacker over the net).
- **Logic Bomb** - malicious code that activates on an event (e.g., date).
- **Trap Door** (or **Back Door**) - undocumented entry point written into code for debugging that can allow unwanted users.
- **Easter Egg** - extraneous code that does something “cool.” A way for programmers to show that they control the product.
Virus Phases

- Dormant phase - the virus is idle
- Propagation phase - the virus places an identical copy of itself into other programs
- Triggering phase – the virus is activated to perform the function for which it was intended
- Execution phase – the function is performed
Virus Protection

- Have a well-known virus protection program, configured to scan disks and downloads automatically for known viruses.
- Do not execute programs (or "macro's") from unknown sources (e.g., PS files, Hypercard files, MS Office documents)
- Avoid the most common operating systems and email programs, if possible.
Virus Structure

program V :=
{
goto main;
1234567;
}

subroutine infect-executable :=
{loop:
  file := get-random-executable-file;
  if (first-line-of-file = 1234567)
    then goto loop
    else prepend V to file; }

subroutine do-damage :=
{whatever damage is to be done}

subroutine trigger-pulled :=
{return true if some condition holds}

main: main-program :=
{infect-executable;
  if trigger-pulled then do-damage;
  goto next;}

next:
}
A Compression Virus

Diagram:

- CV
- $P_1'$
- $P_2$
- $t_0$
- CV
- $P_1'$
- $P_1$
- $P_2$
- $P_2'$
- $t_1$
Types of Viruses

- **Parasitic Virus** - attaches itself to executable files as part of their code. Runs whenever the host program runs.

- **Memory-resident Virus** - Lodges in main memory as part of the residual operating system.

- **Boot Sector Virus** - infects the boot sector of a disk, and spreads when the operating system boots up (original DOS viruses).

- **Stealth Virus** - explicitly designed to hide from Virus Scanning programs.

- **Polymorphic Virus** - mutates with every new host to prevent signature detection.
Macro Viruses

- Microsoft Office applications allow “macros” to be part of the document. The macro could run whenever the document is opened, or when a certain command is selected (Save File).
  - Platform independent
  - Infect documents, not executable portions of code
  - Macro viruses are easily spread, commonly through email
Antivirus Approaches

1st Generation, Scanners: searched files for any of a library of known virus “signatures.” Checked executable files for length changes.

2nd Generation, Heuristic Scanners: looks for more general signs than specific signatures (code segments common to many viruses). Checked files for checksum or hash changes.

3rd Generation, Activity Traps: stay resident in memory and look for certain patterns of software behavior (e.g., scanning files).

4th Generation, Full Featured: combine the best of the techniques above.
Advanced Antivirus Techniques

- Generic Decryption (GD)
  - CPU Emulator
  - Virus Signature Scanner
  - Emulation Control Module

- For how long should a GD scanner run each interpretation?
Malware Examples

■ Email virus – Melissa
  – Made use of Word macros embedded as an attachment
  – Once activated, sent email to everyone on the mailing list of the user’s email package and then did local damage
  – End of 1999, a more powerful version emerged that propagated itself as soon as the email message was opened using the Visual Basic scripting language
Malware Examples

- Morris Worm, 1988
  - Used several propagation techniques: located trusted machines and tried password cracking, bug in the finger protocol, trap door in an email program

- Code Red, July 2001
  - Security hole in Microsoft IIS

- Nimbda, late 2001
RootKit

- Term has been around for 10+ years
- A kit consisting of small and useful programs that allow an attacker to maintain access to “root”
- A Rootkit is a set of programs and code that allows a permanent or consistent, undetectable presence on a computer

Source: Rootkits by Hoglund and Butler
Sony RootKit Case - 2005

- Mark Russinovich detects Sony BMG rootkit-based DRM code
- Sony used software developed at First 4 Internet.
- The software hides the existence of any file, directory, process or registry key whose name begins with "$sys$.
- Russinovich verified this by making a copy of Notepad named "$sys$notepad.exe," which promptly vanished from view.
- Hackers already try to exploit this software
  - World of Warcraft hackers using Sony BMG rootkit
    http://www.ther egister.co.uk/2005/11/04/secfocus_wow_bot/
  - Trojan horse exploits Sony DRM copy protection vulnerability
- Microsoft plans to add this to their list of malware software targeted for removal
- Listen on NPR