

What is a Virus?

- ∅ A program that attaches itself to another **executable** – let's call this a *host program*
- ∅ Whenever a host program is executed, virus code is ran and it can make a copy of itself and infect other executables found in your memory or hard drive
- ∅ Viruses can do any damage they want on your computer

1

Viruses vs. Worms

- ∅ Viruses don't break into your computer – they are invited by you
 - ∅ They cannot spread unless you run infected application or click on infected attachment
 - ∅ Early viruses spread onto different applications on your computer
 - ∅ Contemporary viruses spread as attachments through E-mail, they will mail themselves to people from your addressbook
- ∅ Worms break into your computer using some vulnerability, install malicious code and move on to other machines
 - ∅ You don't have to do anything to make them spread

2

Viruses vs. Trojans

- ∅ Viruses attach themselves to other executables
 - ∅ For example, a Word template or a PowerPoint presentation
 - ∅ They can infect any executable
- ∅ Trojans claim to be other executables but instead contain malicious code
 - ∅ For example, a cool new game is advertised on the Web site but it also contains malicious code
 - ∅ Trojan code will not spread to other programs on your machine, it will simply gain access and do malicious stuff

3

Virus Types

- ∅ **File infectors**
 - ∅ Attach themselves to executable files or even source code
 - ∅ **Direct action** – selects and infects several programs each time host program is run
 - ∅ **Resident** – load themselves into memory whenever a host program is run and then remain in memory infecting any other executable that is executed
- ∅ **System (boot-sector) infectors**
 - ∅ Infect some system area on disk, load themselves on boot and then remain memory-resident
- ∅ **Hybrid**
 - ∅ Infect both files and boot sectors

4

Virus Types

- ∅ **File system (cluster)**
 - ∅ Modify directory table entries so that virus code is loaded and executed before the host program
 - ∅ Host program is not altered, only directory table is
- ∅ **Kernel**
 - ∅ Target specific features of system files

5

Virus Types

- ∅ **Stealth**
 - ∅ Like rootkits
 - ∅ Hide the fact that they have infected the system by modifying replies to system queries
 - ∅ Must be resident
 - ∅ Can only be detected if we boot the system from clean bootable floppy or CD
- ∅ **Polymorphic**
 - ∅ Change virus code to avoid signature detection
 - ∅ Encrypt themselves with variable key – decryption code is always the same
 - ∅ Use different encryption schemes
 - ∅ Encryption + combine NOPs with decryption code

6

Virus Types

- ∅ **Fast infectors**
 - ∅ Infect not only those files that are executed but also those that are merely opened (e.g. by a virus scanner)
- ∅ **Slow infectors**
 - ∅ Only infects modified or newly created files – fools integrity checkers
- ∅ **Sparse infectors**
 - ∅ Infect infrequently (e.g. each 10th file) to avoid detection
- ∅ **Companions**
 - ∅ Creates new file with similar name as the host program
 - ∅ When host program is called, virus is executed instead
 - ∅ Virus calls host program in the end
 - ∅ This fools integrity checkers that only look at existing files

7

Virus Types

- ∅ **Cavities**
 - ∅ Overwrites part of the host program that is filled with a constant
 - ∅ Does not increase the length of host program and preserves functionality
- ∅ **Tunneling**
 - ∅ Some viruses modify interrupt vectors
 - ∅ Tunneling viruses call interrupt handlers directly

8

How Do Viruses Spread?

- ∅ You receive infected E-mail attachment
- ∅ You download infected code
- ∅ Your floppy gets infected

9

What Can Viruses Do?

- ∅ Wipe your hard drive
- ∅ Modify or delete files
- ∅ Steal files
- ∅ Spread further

They frequently delay any malicious actions until they have spread sufficiently

10

Example – I Love You Virus

- ∅ Spreads through E-mail in the attachment containing Visual Basic code
- ∅ When it is executed it copies itself to system directories and modifies registry so that it is automatically restarted on reboot
- ∅ It replaces startup page of Internet Explorer with a download Web page of Trojan code, also adds this program to registry
- ∅ Trojan code is password-stealing code
- ∅ Virus also modifies .vbc, .jpeg, .mp3, etc. files
- ∅ Virus copy will be sent on IRC channels you join
- ∅ Virus also mails its copies to people in your addressbook

Example – Melissa Virus

- ∅ Spreads through E-mail in the attachment named LIST.DOC but can come with other .doc files
- ∅ Spread faster than any other virus known at the time (1999)
- ∅ When it is executed it infects all other .doc files it can find
- ∅ Virus activates if it is executed when day of the month matches the minutes of the hour, e.g. July 1st, 12.01
- ∅ It inserts Simpson's phrase into currently open Word document
- ∅ It can also mail out personal Word documents

12

Example – SoBig Virus

- ∅ Spreads through E-mail in the attachment that contains .pif executable file
- ∅ E-mail addresses are collected from various files on your disk
- ∅ Virus mails itself using its own SMTP engine
- ∅ Also infects system files so that it is restarted on reboot
- ∅ Virus downloads backdoor code from a Website

13

Indicators of Virus Infection

- ∅ Changes in file sizes or checksums
- ∅ Unaccounted resource consumption
- ∅ Changes of interrupt vectors
- ∅ Best detection would be to analyze all files on your system for modifications – impractical

14

Virus Detection Systems

- ∅ **Activity monitoring systems**
 - ∅ Look for virus-like activity such as trying to overwrite other executable files, attempts to reformat disk, etc.
 - ∅ May generate false positives
- ∅ **Scanners**
 - ∅ Look for patterns in virus code
 - ∅ Use database of known virus signatures
 - ∅ Detect polymorphic variations
 - ∅ Sometimes they use heuristics to detect new virus signatures
 - ∅ Most scanners also include disinfection code
 - ∅ Must encode virus strings to avoid false positives
- ∅ **Integrity checkers**
 - ∅ Detect file modifications

15

Virus Detection Systems

- ∅ Usually resident
- ∅ Sometimes can even be added to boot sector to detect boot sector viruses
- ∅ Some virus detection systems will prohibit access to floppies unless they have been scanned before
- ∅ Or they will encrypt executable files

16

Virus Detection Hardware

- ∅ Defines non-writable areas of the disk for executable files
- ∅ Sounds alarm and/or requires password in order to modify these areas
- ∅ Might be annoying and generate false alarms

17

Virus Removal

- ∅ Identify which files have been modified
 - ∅ Virus scanners will do this
- ∅ Restore last known good copy of these files from your backup
- ∅ It is not necessary to re-format the disk
- ∅ Some virus scanners can disinfect files – remove the virus code

18

Can a Virus Infect Data Files?

- ∅ Yes, but it will never be executed because data files do not contain executable code
- ∅ Virus can be hidden in .gif and .jpeg files using steganography but it has to be extracted and run by an executable

19

Can a Virus Spread To Other OS?

- ∅ No, virus contains OS specific code
- ∅ You may receive virus on another OS but it won't run and therefore won't spread
- ∅ How about worms?

20

Can a Virus Infect Mainframe Computers?

- ∅ Yes but it's harder
- ∅ Mainframe computers have write protections among users so virus can only infect user A's files
- ∅ However if user A sends his file to user B then B's files also get infected
- ∅ If virus is placed in shared area then all user's files may get infected
- ∅ Mainframe computers are generally better maintained and it is hard to write a good mainframe virus – only a few exist so far

21

How About Self-Checking Code?

- ∅ Add an integrity-checking code to every file so that it checks whether it is infected every time it is run
- ∅ If the file is infected virus will be executed first
- ∅ It can also fiddle with integrity-checking code and disable it
- ∅ Ineffective against companion viruses

22

Virus Simulators

- ∅ Demonstrate audio and visual effects of some computer viruses
- ∅ Create virtual environment and virtual viruses so users can observe the spread without getting infected
- ∅ Generate artificial strings that appear in viruses but don't spread and don't take any malicious action
- ∅ Used for educational purposes or to test antivirus software

23

Why Are Viruses Perceived As Harmful?

- ∅ They spread beyond our control – there is no way to stop the spread of a virus that you release
- ∅ It is hard to distinguish between viruses and benign code
- ∅ They eat resources
- ∅ They may do malicious things
- ∅ They may disable self-checking program
- ∅ They may infect hospital computers and do irreparable damage

24

How About Good Viruses?

- ∅ People have toyed with the idea of useful viruses but this has not been accepted
 - ∅ Virus idea simply seems to be dangerous
 - ∅ Good virus code may be buggy and thus vulnerable
 - ∅ Good virus could ask for permission to infect the system –
Imagine this scenario on a hospital computer
 - ∅ Bad virus code could be attached to a good virus to slip detection
 - ∅ Legal issues might arise
 - ∅ People don't like the idea²⁵ that someone takes control

What Would Good Viruses Do?

- ∅ Detect viruses and fix infected files
- ∅ Compress files and decompress them at run time
- ∅ Encrypt hard drive and require user password for decryption
- ∅ Maintain machines, e.g. delete temporary files – comes by invitation
- ∅ People haven't been able to come up with a controlled way to plant a good virus
 - ∅ Asking for acceptance wastes (maybe precious) time
 - ∅ Checking for invitation wastes resources
- ∅ People haven't come up with a compelling use of a good virus