

Viruses, Trojan Horses, Worms, etc.

- Resources

- <http://www.wildlist.org/>
- <http://www.iwar.org.uk/comsec/>
- "Viruses Revealed" by Harley, Slade and Gatticker, McGraw-Hill
- "Modern Operating Systems," by Tanenbaum



Virus researchers owe this man a debt of gratitude



COMP 6370 – Lecture 5 – Malicious Software



The three pillars of Information Security

- **Confidentiality:** protecting information from unauthorized disclosure;
- **Integrity:** protecting information from unauthorized modifications, and ensure that information is accurate and complete;
- **Availability:** ensuring information is available when needed;



COMP 6370 – Lecture 5 – Malicious Software



Direct Damage from Virus & Trojan Payloads

- **Availability**
 - Deletion of files and directories
 - Renaming of files
 - Encryption of files, disks, system calls
 - Unauthorized calls to system software such as FORMAT, FDISK, etc.
- **Integrity**
 - Corruption of system files and system areas (MBRs, FAT, etc.)
 - Garbling data such as spreadsheet formulas...
 - Corruption of both application and data files by unauthorized file writes
- **Confidentiality**
 - Capture and forwarding of passwords
 - Forwarding of personal and confidential files to newsgroups and elsewhere



COMP 6370 – Lecture 5 – Malicious Software



Hacking is actually NOT resume building



COMP 6370 – Lecture 5 – Malicious Software



Defining a Computer Virus

- A virus is an entity that uses the resources of the host to spread and reproduce itself, usually without informed operator action.
- A virus cannot execute on its own.
- Strong viruses use normal computer operations to achieve the virus design goals.
- *There is no single characteristic that can be used to identify a previously unknown virus program.*
- Consequently, there is some academic disagreement as to just how many viruses have been released, what variants define different strains.



COMP 6370 – Lecture 5 – Malicious Software



Virus Structure

- **Infection:** The infection mechanism may be defined as the way or ways in which the virus spreads.
- **Payload:** The payload mechanism is defined as what (if anything) the virus does *in addition* to replicating.
- **Trigger:** The trigger mechanism is defined as the routine that decides what time to deliver the payload if there is a payload.



COMP 6370 – Lecture 5 – Malicious Software



Virus Damage

- **Deliberate damage** inflicted by the virus payload mechanism, if it exists, such as the trashing or intentional corruption of files.
- **Accidental damage** caused when the virus attempts to install itself on the victim system (the newly infected host), such as corruption of system areas preventing the victim system from booting.
- **Incidental damage** that may not be obvious but is nevertheless inherent in the fact of infection. Nearly all viruses entail damage in this category, since their presence involves loss of performance due to theft of memory, disk space, clock cycles, system modifications or combination of these,



COMP 6370 – Lecture 5 – Malicious Software



7

Some Social Impacts

- Scapegoating of virus victims
- Secondary damage to systems caused by inappropriate responses to a perceived virus threat (ex. low-level formatting of a hard disk to eradicate a macro virus.)
- Legal or quasi-legal issues such as failure to comply with data-protection legislation and policies.
- Inappropriate security responses
 - reformatting
 - passwords
 - change in business models



COMP 6370 – Lecture 5 – Malicious Software



8

A Few Examples of Virus Damage

- The disappearance of Word menu options relating to the presence of macros.
- Encryption or displacement of system areas, such as the Master Boot Record.
- Manipulation of the Windows Registry
- Trashing or corruption of legitimate macros as part of the installation of a macro virus.



COMP 6370 – Lecture 5 – Malicious Software



9

Latency

- Unexecuted viruses are latent or dormant
 - ex. mailbox full of unread, infected mail
 - ex. PC-specific virus residing on a Mac or a UNIX server.
- “Heterogeneous virus transmission.”



COMP 6370 – Lecture 5 – Malicious Software



10

Some Useful Terms

- **Intendeds**: reproductive mechanism never triggers, or if triggered, code never attaches to host.
 - ex. virus intended to execute on Sundays and uses DOS system call Get Date. Virus waits for Get Date to return “7” but Get Date only returns values between “0..6.”
- **Corruptions**: may be caused by system transfers, incomplete “cleansing” and poorly maintained virus collections.
 - Antivirus programs often detect corrupted non-viral programs simply to avoid being penalized by incompetent testers and reviewers.



COMP 6370 – Lecture 5 – Malicious Software



11

Virus Design Considerations

- Polymorphic Viruses – change structure in attempts to avoid detection
- Non-Resident (direct action) versus Memory-Resident viruses.
 - Hybrids
 - Macros
- Payload versus reproduction
- Damage
 - In general, a virus can do anything any other software can do
- Boot Sector



COMP 6370 – Lecture 5 – Malicious Software



12

Attaching viral code to an existing program

- Overwrite existing program code (overwriting viruses)
- Add code to the beginning of the program (prependers)
- Add code to the end of the program (appenders)
- Insert viral code into the command chain so that it is run when the legitimate code is executed (parasitic viruses or file infectors)
 - Macro viruses are a special case of a file infector
- These methods are becoming less common as VBScript, AOL programs and MS Office macros continue to ease the task of virus writers.



COMP 6370 – Lecture 5 – Malicious Software



13

Polymorphic Virus Techniques

- **Objective:** fool scanners, make signatures harder to identify
- **Methods**
 - Encryption: Start with a "random" number such as the value of seconds in system time then use that as a key to encrypt part of the payload.
 - Arbitrary code relocation: rearrange code after each infection.
- **Detection**
 - change detection
 - activity monitoring
 - detecting the mutating engine in kit-produced viruses
 - bankruptcy of scanners that cannot detect polymorphic viruses



COMP 6370 – Lecture 5 – Malicious Software



14