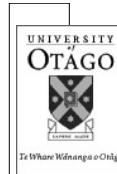


COMP201

Computers For Professionals



Viruses and Worms



Viruses and Worms



- Have you ever caught a virus?
 - When did you last run a virus checker?
 - When did you last update your virus checker?
- Have you ever been attacked by a worm?
 - Do you use a firewall?
 - When did you last update your firewall?
- Do you have a backup of all your important data?



Virus Definition



- *“a self-replicating computer program that spreads by inserting copies of itself into other executable code or documents”*
(Wikipedia entry for “Computer virus”)
- From biology:
 - The inserted code is called the ***virus***
 - The infected file is called the ***host***
 - Insertion of the virus is called ***infection***



Virus Infection



- Boot sector viruses
 - When a disk is booted the virus is loaded with the operating system and remains in memory
- Program viruses
 - When a program is loaded into memory the virus is loaded and remains in memory
- Macro viruses
 - When a data-file (e.g. word document) is loaded a virus in the file is loaded and remains in memory

Virus Replication



- Boot sector viruses
 - When a disk read or write occurs the virus also writes itself to the disk (undetected) – in this case the boot sector of any attached disks
- Program viruses
 - When a user loads a program the virus attaches itself to the other programs on the disk
- Macro viruses
 - Saved with all documents (and templates) saved after the infection has occurred

Virus Activation



- Many virus carry a destructive payload (a **bomb**)
 - Display a message on a given day
 - Delete files
 - Delete the operating system
- Time bombs
 - Occur on a specific date and time
- Logic bombs
 - Occur when the user performs some specific action
- The overwhelming **annoyance** is the infection of files that must later be cleaned

Virus Pandemic



- Boot sector viruses
 - An infected disk is booted on a clean computer
- Program viruses
 - File servers
 - Programs downloaded from the internet (kracks)
 - “Sharing” programs
- Macro viruses
 - Email
 - File servers
- Viruses spread because they are carried by people from one computer to another

Detection



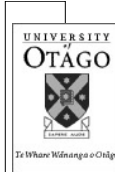
- Viruses are just computer programs!
- Signature
 - The parts of the program unique to the virus
- Anti-virus programs scan for known signatures
 - On detection, the virus can often be removed
 - Only known signatures can be detected
- Keep the signature list up-to-date
 - Download the latest release from the vendor



Cleanup



- Remove the virus
 - Reconstruct the boot-sector
 - Remove the virus from the program
 - Remove the macro from the data files
- Reconstruct the original files (undamage?)
 - This is often not possible
 - Undelete deleted files?
 - Re-write scrambled word and excel files?



Stories



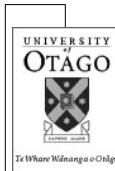
- Read the story of a typical virus outbreak, the containment, disinfection, and responsibilities (\$250,000 damage in his case):
 - <http://www.cio.com/archive/060101/outbreak.html>
- Ask yourself:
 - Is the virus author responsible?
 - Is the Chief Information Officer (CIO) competent?



More About Viruses



- Non-resident viruses
 - Some viruses live outside of memory
 - Load, Replicate, Unload
- Piggy-back on the virus software (stealth)
 - Some look for virus detectors and modify them
- Mutating viruses
 - Some viruses mutate to avoid being found
- No operating system is immune
 - Mac / Linux / Windows
 - The first released virus was on the Apple []
- Damage worldwide is high
 - \$17 Billion in 2000



Worms



- The main difference between a computer virus and a worm is that a virus cannot propagate by itself whereas worms can. A worm uses a network to send copies of itself to other systems and it does so without any intervention.
- In general, worms harm the network and consume bandwidth, whereas viruses infect or corrupt files on a targeted computer.
(Wikipedia entry for "Computer virus")

The Underground



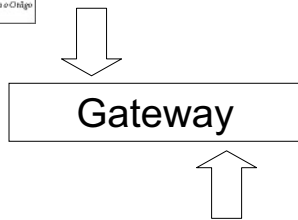
- Some worms install **backdoors**
 - Mail sender for sending spam
 - Packet sniffers
 - Key loggers
- Spammers are thought to fund such worms
- Worm writers sell lists of infected machines
- Some companies have been blackmailed with threats of DoS attacks

Beneficial Worms?



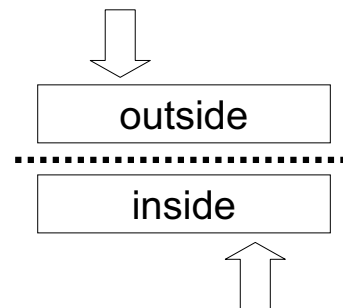
- The **Nachi** family of worms propagated through holes in Windows, then download any patches (from Microsoft) to fix the vulnerability!
- The hosts were better defended and more resilient to attack, but generated network traffic (more than the worms they protected against!)
- They did this without consent from the owner!

Worm Protection



A **gateway** allows data to pass from one network to another.

A **firewall** filters the data before transferring it. Only passes authorized traffic (e.g. email, Web)



Things to Remember



- Install (and use) anti-virus software
 - Periodically up-date your anti-virus program
 - Every new release
- Install operating system patches
 - Prevent new infection through old holes
- Install (and use) a firewall
 - Keep it up-to-date too as firewalls can be attacked
- Remember!
 - No operating system or software is immune