Viruses, Worms and Trojans

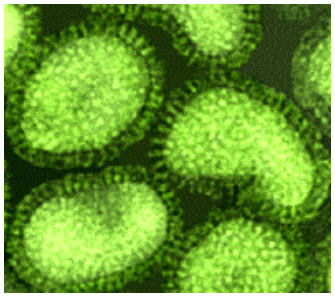
Dr George R S Weir

gw@cis.strath.ac.uk

Outline

- The nature of viruses, worms & Trojans
- Brief history
- Examples
- Survival strategies

A common virus…



influenza

A common worm…

earth worm

A real Trojan horse…

Viruses are unwelcome

- viruses are unwanted infestations
- they usually have undesirable side-effects
  - e.g., file deletion or password collection
- usually have the capacity to spread copies of themselves to other computer systems
- they are malicious programs
- often designed to remain hidden and use all available means to spread

Viruses come in many varieties

- viruses differ in their behaviour
- some display messages
- others are more malicious
  - e.g., targeting and deleting specific types of files
- some are more dangerous and will reformat hard disks on an infected machine
- the intended action of any virus is termed the 'payload'
- this is what the virus can do on an infected machine

Execution environment

- another significant feature of any virus is the environment it needs in order to effect its behaviour
- a virus is merely a software program
- there must be an execution environment that will support the running of the virus program
- this is an inescapable truth for all types of virus

Viruses and their relatives

- viruses differ from worms and Trojans
- but many instances cross the defining boundaries of each type
- the defining characteristic of a virus is its capacity to spread copies of itself
- early viruses used modem links to cross networks
- later viruses were mainly spread through contamination of boot disks
- the ability to spread by means of network links is a defining feature of a worm

Viruses and their relatives (2)

- so a virus that spreads across networks, either by modem or via Internet email is also a worm
- worms may derive their name from the idea of programs wriggling from one location to another
- an unwelcome program that infects a disk boot sector and spreads by exchange of infected floppy disks is usually not a worm
  - but is still a virus
- a Trojan is a program that conceals its true nature
  - pretending to be something innocent
  - but it may be malicious
  - and may contain a worm virus

Trojans

- named after the wooden horse in Greek mythology
- Trojan programs are often used to carry viruses or worms
- one variety might be hidden in software such as games or graphics software
  - unlikely if the software is from a reputable source
- others simply pretend they are innocuous or useful programs
- but when executed innocently by the user take their full effect

Characteristics

Program Type	Feature				
	Self Replicates	*Concealment*	*Spreads by networks*	*Damaging payload*	*Apparently safe*
Virus	Yes	Yes	Sometimes	Often	Sometimes
Worm	Yes	Yes	Yes	Usually	No
Trojan	Yes	No	Often	Yes	Yes

Earliest computer virus?

- Popular contenders are ‘Christmas Tree’ and ‘Pervading Animal’
- appeared in the late 60s on the Univac 1108 system and the IBM 360/370 systems

Univac 1108 (circa 1968)

Virus history

- in the mid 70s came the ‘creeper’ virus
- the Creeper was a program designed for demonstration that ended up going out of control
- it crawled through the ARPAnet (pre-Internet), across university, military, and corporate computers
- leaving a message wherever it appeared:
  “I’m the Creeper, catch me if you can”
- this program was able to transfer itself to other networks by modem
  - so it was also a worm

The reeper

- the Creeper was also the reason for creating the first anti-virus program: the ‘Reeper’
- the Reeper behaved like the creeper
- travelling from machine to machine, but it eliminated any copies of the creeper that it found
- by the 80s the popularity of personal computers led to a vast increase in the incidence of computer viruses

Virus varieties

several distinct varieties of virus:

- **Boot sector viruses**
- **File viruses**
- **Logic bombs**
- **Macro viruses**

Boot sector viruses

- attack the boot sector or the master boot record
- overwrite the original code and replace it with the infected code
- **copied from one machine to another** via floppy disk
- a floppy disk read on an infected machine has a copy of the boot sector virus copied to the boot sector of the floppy disk
- this floppy is later read on a clean computer, the virus copies itself to the boot sector of the new machine’s hard disk and the whole cycle can begin again

Boot sector viruses (2)

- for boot sector viruses the **execution facility** lies in the reading of the disk's boot sector
- the OS reads and executes the code it finds in the boot sector
- a further copy of the virus is placed into memory on the computer
- from where it continues to infect other disks or to re-infect its own hard disk against weak attempts to clean the infection
- boot sector viruses can also infect the boot sectors CD-ROMs and DVD-ROMs

The Michelangelo virus

- one well-known boot sector virus is the Michelangelo virus
- first circulated in 1991 with a vicious payload
- on Michelangelo's birthday (6 March), the virus would wipe the hard disk of any infected machine
- the Michelangelo type of virus is also known as a 'logic bomb'

File viruses

- file viruses employ a different strategy
- they conceal themselves by attaching to existing executable files on the user's computer
- this makes the virus invisible to casual inspection
- only expected file names will be revealed in a typical system scan
- when an infected executable file is run, the added virus code is also executed
- this allows the virus to deliver its payload, including affecting other files

Logic bombs

- A favourite of disgruntled employees and computer extortionists
- logic bombs are destructive programs with a timer or trigger to set it off
- may have no other virus qualities
- or may be like the Michelangelo virus

Macro viruses

- a common variety of virus
- infects software packages such as the 'MS Office' suite of programs
- a macro is a set of instructions within an application that can be used to automate tasks
- macro viruses are unwanted macros that execute in the environment of an application such as Word, Excel, PowerPoint or Access
- this means they will execute sets of scripts or instructions (the macros) attached to data files
- these Office applications are closely linked to the operating system, and can make changes to files or delete existing files

The Concept virus

- earliest macro virus was the 'concept' virus
- first encountered in August 1995
- several large companies began meeting the nuisance of a MS Word macro that copied and reproduced itself
  - also accidentally distributed on CD-ROM by Microsoft at a trade fair (allegedly!)
- this macro infection had no malicious payload
- but it did display a message from the author: "That's enough to prove my point"

Polymorphic viruses

- polymorphic viruses are designed to hide from anti-virus programs by changing slightly each time they are executed
- a polymorphic virus was first created by Mark Washburn, who modified the source for a virus called 'Vienna' to change itself
- this example was not very infectious and made little impact
- a widely encountered polymorph was called Tequila
- Tequila originated in Switzerland and was spread through shareware
- Tequila was fully polymorphic, meaning that no search string can be guaranteed to detect such a virus
- this was a new problem for anti-virus software to deal with and it took several months to get the better of Tequila

Worms

- most recent viral activity involves worms infecting PCs running MS-Windows
- many such worms also qualify as Trojan horses
- they often portray themselves as harmless screensavers or helpful information in executable files
- another common characteristic of modern worms is that they are often macro viruses

Worms (2)

- worms may use 'social engineering' to have users execute unsafe code
- a malicious program may be attached to email messages that entice recipients to execute the program
  - by suggesting that it contains a love letter or some other delight
- the executable attachment is simply a means of having users execute the malicious code
- such worms then spread to other locations
- the worm may hijack the user's own email facility
  - send copies of itself as attachments to all addresses in the user's address book
- since the email messages then arrive from a known sender, this increases the likelihood that new recipients will trust the attachment and that it will continue to spread

Example worms

- many recent examples of worms including Melissa' and the 'I love you' (lovebug worm)
- the lovebug worm was a 37 line Visual Basic program
- when executed on a Windows PC, it created a message with the Subject: 'ILOVEYOU' and the body: 'kindly check the attached LOVELETTER coming from me'
- this message was then sent to every address in the user's email address book
- this worm and many others, rely on the presence of specific mail programs, usually Outlook and Outlook Express

Trojan worm

- worms such as 'ILOVEYOU' also qualify as Trojans
- they masquerade as an innocent item that the user is 'suckered' into executing
- other worms use more subtle means to execute
- the Nimda worm was another mass-mailing worm that used a variety of transfer methods
  - incidentally, the virus took its name from the reversed spelling of 'admin'

Blaster

- the Blaster worm exploits vulnerability in the implementation of Microsoft's Remote Procedure Call (RPC) program
- the worm targets only Windows 2000 and Windows XP computers
- it uses the system flaw to download a file called Mslaugh.exe into the Windows system folder and then execute it
- the worm then scans the Internet for other computers that can be infected in the same way

More Trojans

- one sub-category of Trojan makes it possible for someone else to access your computer over the Internet
- this type of program is called a 'backdoor'
- such Trojans may be attached to other executables (a file virus) or may be 'built-in' to a freely distributed software program (e.g., a useful free or shareware utility)
- the Trojan may be transferred and executed when you visit a Web site that offers to download and install a feature for you
- finally, the Trojan may be transferred and executed by unsuspecting email recipients (as an executable file attachment)

Backdoors

- Trojans that provide backdoor access to a computer system have a server and a client part
- the server program is the Trojan horse that infects your computer
- this runs on your machine and provides access into your computer
- the client program is used by someone externally to communicate with the server program and break into your computer

Backdoor Trojans

- one example is the GirlFriend Trojan
- this uses communication port 21554
- an external user may scan your computer across the network to see whether port 21554 responds
- if port 21554 is accessible and you are running the GirlFriend Trojan, the hacker can access your computer

BackOrifice

- many Backdoor threats are derived from the notorious program BackOrifice
- this was released by a group of hackers calling themselves 'the Cult of the Dead Cow'
- they aim to point out the vulnerability of Windows operating systems
- the BackOrifice Trojan waits for incoming connections on a preconfigured port through which an attacker can:
  - upload and download files
  - start programs
  - delete files
  - shut down the computer
  - lock you out of the computer
  - take control of the mouse and keyboard

Beating viruses, worms and Trojans

- knowledge is the best defence
- try to keep up to date with current developments
- understand the mechanism used by such programs…

Three vitals

How your machine gets contaminated (e.g., email, network share, port vulnerability…)

How the intruder executes on your machine (e.g., email attachment, Trojan, system vulnerability…)

What the intruder does to your machine (e.g., sending email, deleting files, infecting other machines)

Defences

- the characteristics of viruses, worms and Trojans may vary widely
- differing strategies are essential for defending computers against such infections
- appropriate measures for removing existing infections may not be adequate to protect against future attacks
- a regularly updated anti-virus program is essential for any network-enabled computer
- this is especially true for Windows machines, since these are the more common target for attack

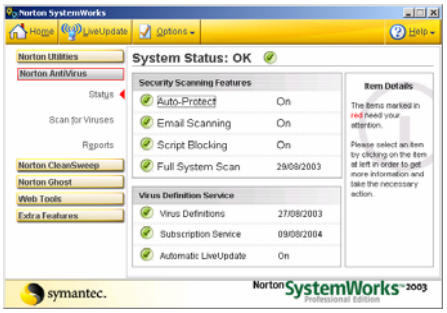
Anti-virus programs

- contain a generic scanning engine that can search and analyse the files contained on the host machine
- other prime indicators, such as Windows registry entries, may also be scanned.
- the anti-virus scanner operates in conjunction with a database of viruses, worms and Trojans
- this data identifies the key features (fingerprints) that characterise each infection
- the scanner checks each file and registry entry against the database information
- if an infection is detected, the anti-virus engine can attempt to remedy the situation by repairing the file, deleting the file, or by placing the suspect files in a quarantine location

Protection

- additional measures are required to maintain immunity from attack
- most anti-virus programs require regular updates to the local database of virus definitions
- this enables the scanner to call upon the latest insights into virus fingerprints
- some anti-virus programs have an update facility in-built
- this makes for easy access to the latest virus definitions and may also allow for upgrades to the scanning engine itself

Norton Systemworks



Other precautions

anti-virus programs may also

- check files downloaded from the Internet
- check the integrity of email (both incoming and outgoing) to ensure that no worms, Trojans or other viruses are deposited or relayed to other locations

Guarantees?

- there is no guarantee that infection cannot occur
- there are several contexts in which problems may still arise
- new strains of virus, worm and Trojan are constantly being released
- anti-virus software tries to keep up
- some sites will be infected by new variants before they can be diagnosed and fingerprinted for anti-viral measures
- also anti-virus software cannot prevent gullible users from executing new Trojan horse programs

Other risks

- presently unknown vulnerabilities in computer operating systems cannot be secured in advance
- software firewalls afford some additional measure of protection against such remote exploits

Hoaxes

- don't be taken in by emails advising you to tell everyone you know about a new virus
- always check the truth of such alarms at a trusted anti-virus site

Stay safe and avoid…

viruses

worms

Trojans