CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Malicious Software and Denial of service attacks

Viruses

Video Summary

- What is a Virus?
- Nature of Viruses
- Compression Virus
- Virus Classifications
- Macro-virus (Melissa)

Viruses

- Piece of software that infects programs
  - Modifies them to include a copy of the virus
  - Replicates and goes on to infect other content
  - Easily spread through network environments

- When attached to an executable program a virus can do anything that the program is permitted to do
  - Executes secretly when the host program is run

- Specific to operating system and hardware
  - Takes advantage of their details and weaknesses

Nature of Viruses

- A virus is piece of software that “infects” programs and copies itself to other programs
- The phases of a virus are:

Nature of Viruses

- A virus is piece of software that “infects” programs and copies itself to other programs
- The phases of a virus are:
    1. Dormant: virus is idle; will be activated by some event (like logic bomb)

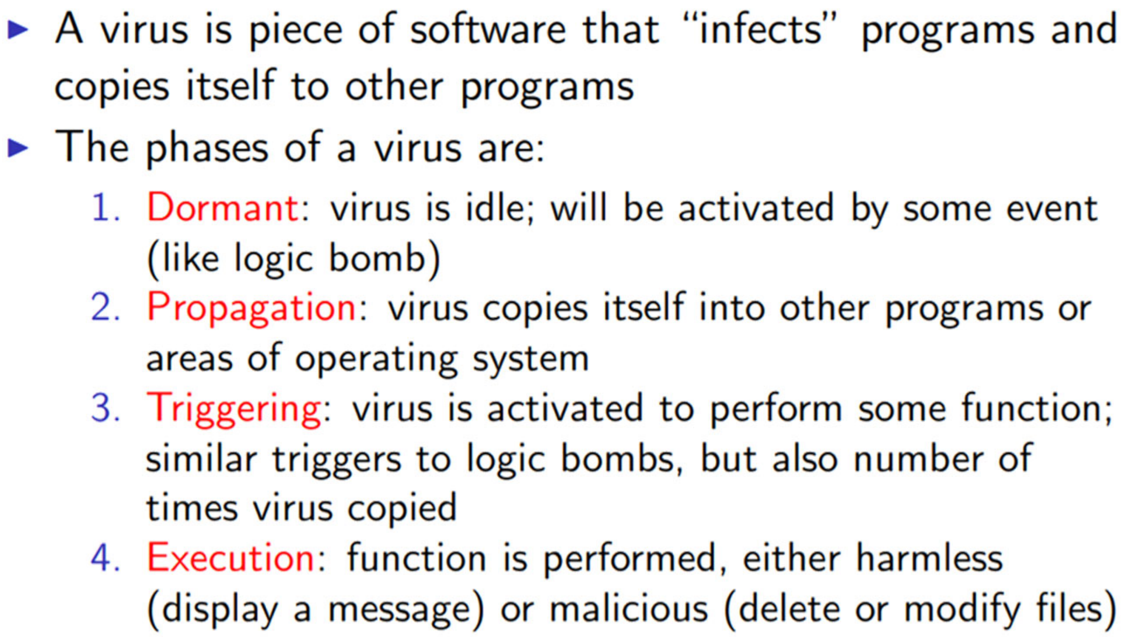
Nature of Viruses

- A virus is piece of software that “infects” programs and copies itself to other programs
- The phases of a virus are:
  1. Dormant: virus is idle; will be activated by some event (like logic bomb)
  2. Propagation: virus copies itself into other programs or areas of operating system

Nature of Viruses

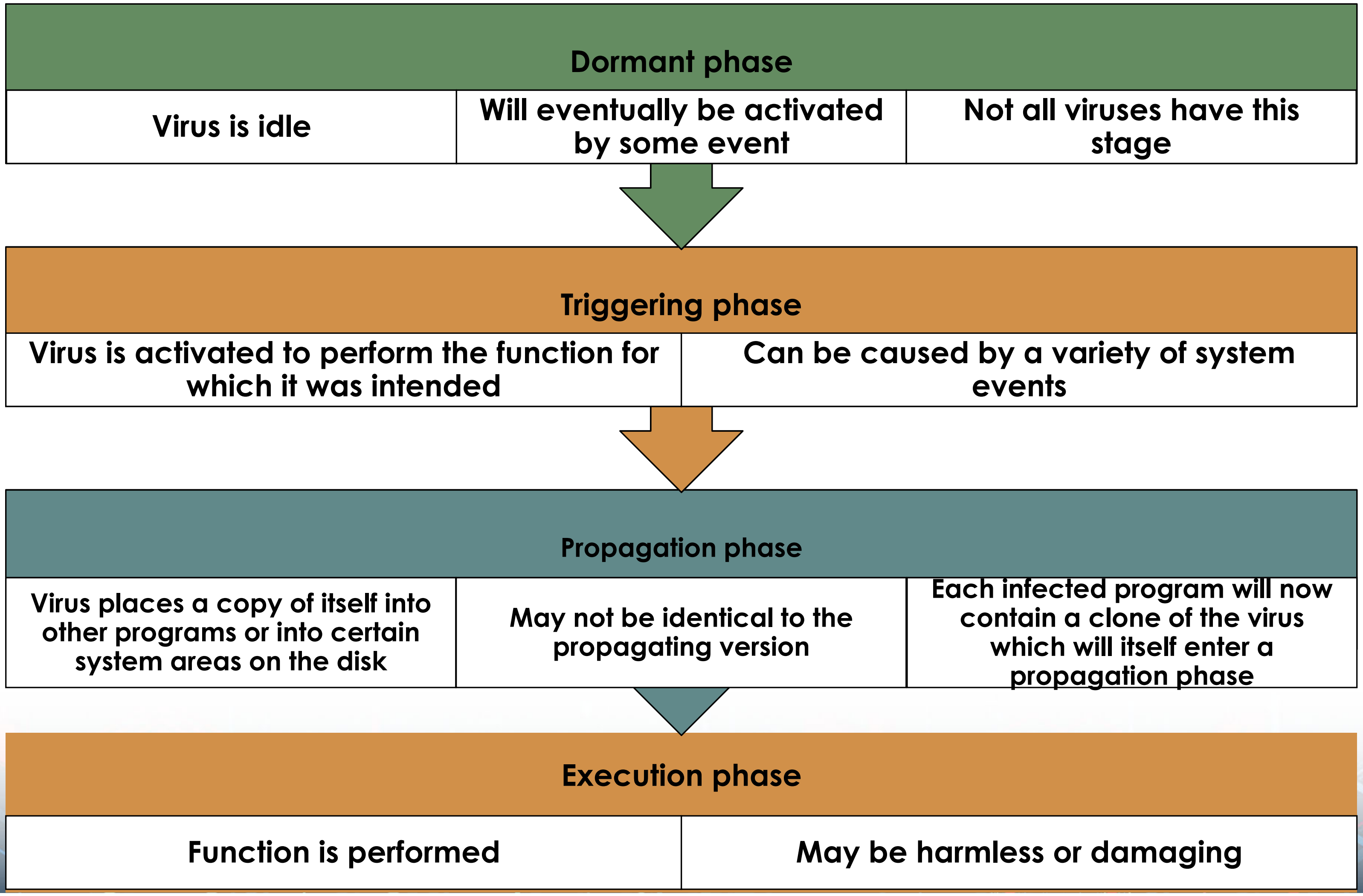
- A virus is piece of software that "infects" programs and copies itself to other programs
- The phases of a virus are:
  1. Dormant: virus is idle; will be activated by some event (like logic bomb)
  2. Propagation: virus copies itself into other programs or areas of operating system
  3. Triggering: virus is activated to perform some function; similar triggers to logic bombs, but also number of times virus copied

Nature of Viruses



- A virus is piece of software that "infects" programs and copies itself to other programs
- The phases of a virus are:
  1. Dormant: virus is idle; will be activated by some event (like logic bomb)
  2. Propagation: virus copies itself into other programs or areas of operating system
  3. Triggering: virus is activated to perform some function; similar triggers to logic bombs, but also number of times virus copied
  4. Execution: function is performed, either harmless (display a message) or malicious (delete or modify files)

Virus Phases



Dormant phase

Virus is idle

Will eventually be activated by some event

Not all viruses have this stage

Triggering phase

Virus is activated to perform the function for which it was intended

Can be caused by a variety of system events

Propagation phase

Virus places a copy of itself into other programs or into certain system areas on the disk

May not be identical to the propagating version

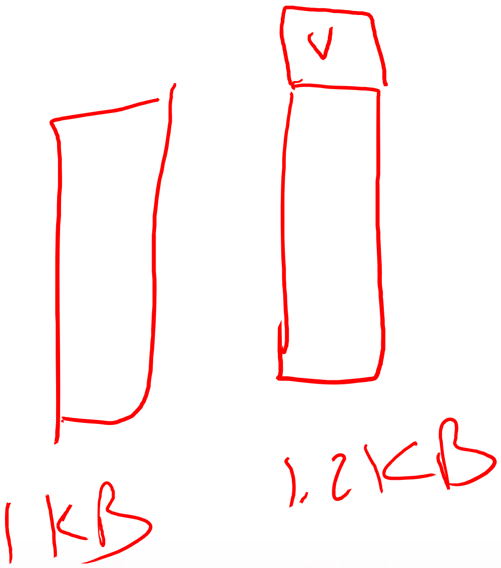
Each infected program will now contain a clone of the virus which will itself enter a propagation phase

Execution phase

Function is performed

May be harmless or damaging

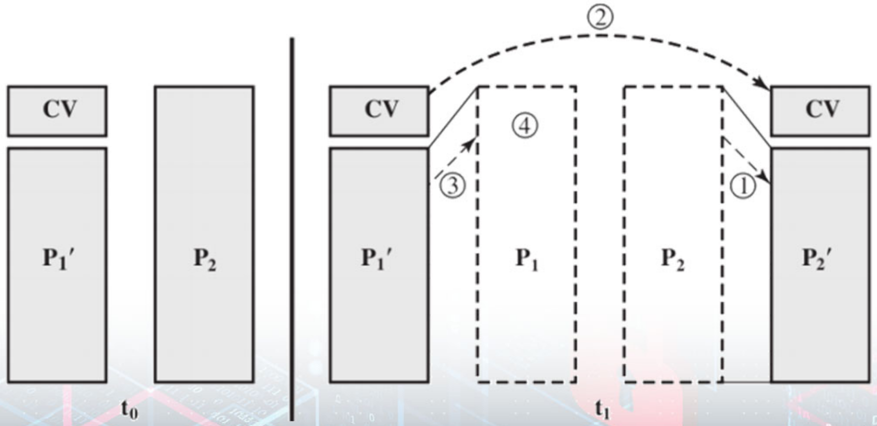
A Simple Virus

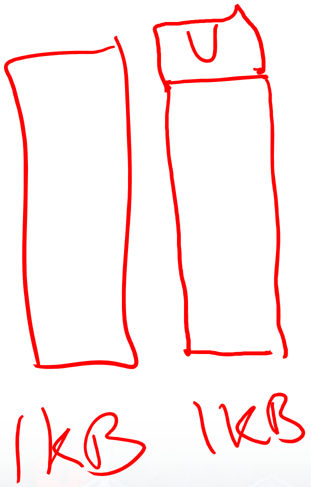


```
program V :=
{goto main;
   1234567;
   subroutine infect-executable :=
      {loop:
      file := get-random-executable-file;
      if (first-line-of-file = 1234567)
         then goto loop
      else
         prepend V to file; }
   subroutine do-damage :=
      {whatever damage is to be done}
   subroutine trigger-pulled :=
      {return true if some condition holds}
main: main-program :=
   {infect-executable;
   if trigger-pulled
      then do-damage;
   goto next;}
next:
}
```

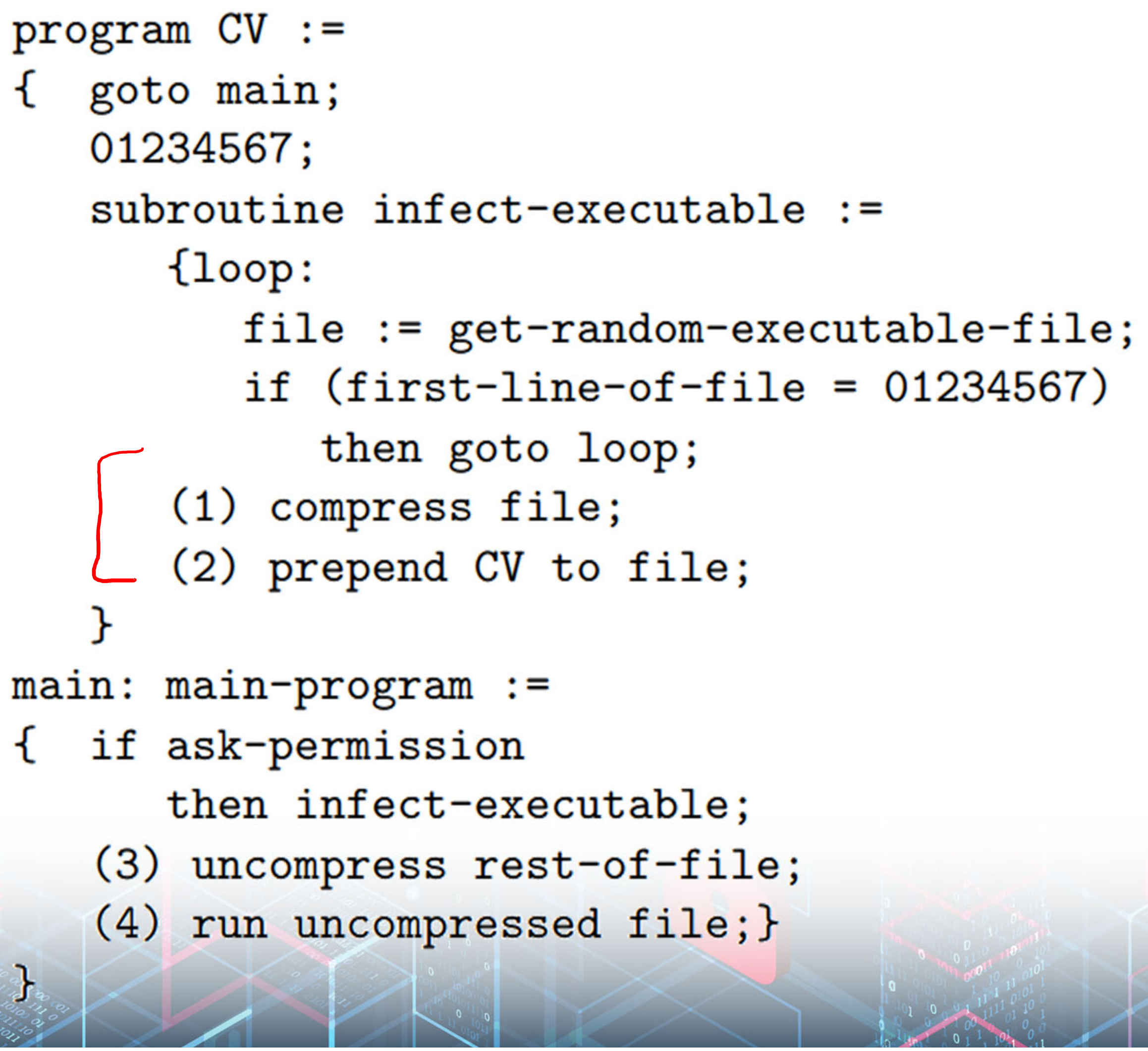
Compression Virus

- The simple virus can be detected because file length is different from original program
- This detection can be avoided using compression
- Assume program P1 is infected with virus CV
  1. For each uninfected file P2, the virus compresses P2 to produce P2
  2. Virus CV is pre-pended to P2 (so resulting size is same as P2)
  3. P1 is uncompressed and (4) executed





Compression Virus



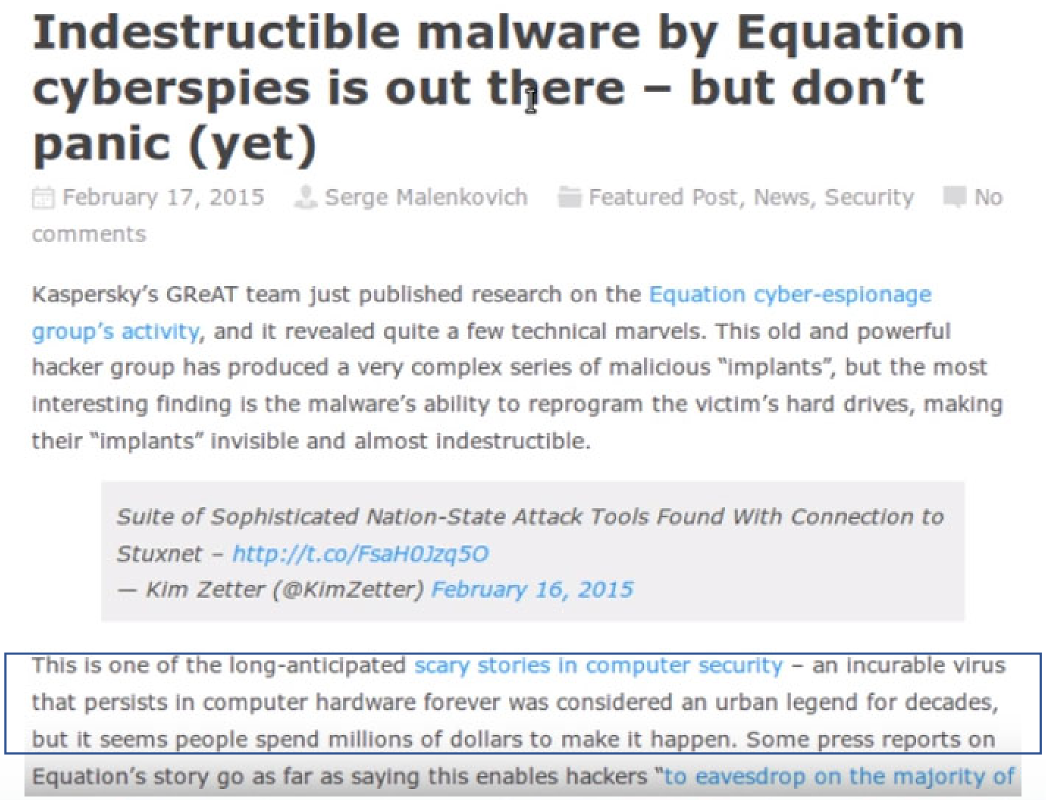
```
program CV :=
{   goto main;
    01234567;
    subroutine infect-executable :=
        {loop:
            file := get-random-executable-file;
            if (first-line-of-file = 01234567)
                then goto loop;
        (1) compress file;
        (2) prepend CV to file;
    }
main: main-program :=
{   if ask-permission
        then infect-executable;
    (3) uncompress rest-of-file;
    (4) run uncompressed file;}
}
```

Virus Classifications

- Classification by target
  - Boot sector infector
    - Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus
  - File infector
    - Infects files that the operating system or shell considers to be executable
  - Macro virus
    - Infects files with macro or scripting code that is interpreted by an application
  - Multipartite virus
    - Infects files in multiple ways

- Classification by concealment strategy
  - Encrypted virus
    - A portion of the virus creates a random encryption key and encrypts the remainder of the virus
  - Stealth virus
    - A form of virus explicitly designed to hide itself from detection by anti-virus software
  - Polymorphic virus
    - A virus that mutates with every infection
  - Metamorphic virus
    - A virus that mutates and rewrites itself completely at each iteration and may change behavior as well as appearance

Hard disk Firmware Virus



Indestructible malware by Equation cyberspies is out there – but don't panic (yet)

February 17, 2015 Serge Malenkovich Featured Post, News, Security No comments

Kaspersky's GReAT team just published research on the Equation cyber-espionage group's activity, and it revealed quite a few technical marvels. This old and powerful hacker group has produced a very complex series of malicious "implants", but the most interesting finding is the malware's ability to reprogram the victim's hard drives, making their "implants" invisible and almost indestructible.

> *Suite of Sophisticated Nation-State Attack Tools Found With Connection to Stuxnet – http://t.co/FsaH0Jzq5O*
> *— Kim Zetter (@KimZetter) February 16, 2015*

This is one of the long-anticipated scary stories in computer security – an incurable virus that persists in computer hardware forever was considered an urban legend for decades, but it seems people spend millions of dollars to make it happen. Some press reports on Equation's story go as far as saying this enables hackers "to eavesdrop on the majority of

μc.

Macro and Scripting Viruses

- NIST-IR 7298 defines a macro virus as: → word excel

  “a virus that attaches itself to documents and uses the macro programming capabilities of the document’s application to execute and propagate”

- Are threatening for a number of reasons:
  - Is platform independent
  - Infect documents, not executable portions of code
  - Are easily spread
  - Are much easier to write or to modify than traditional executable viruses

Macro-Virus (Melissa)

- Virus released by David Smith in 26 March 1999
- Posted a message to a newsgroup containing an MS Word attachment (macro-virus)
- Estimated damage up to $1000 Million
- Designed to infect computers with Word 97/2000

Macro-Virus (Melissa)

- Virus sent as attachment to email:
  - Subject: “Important message from <user name>”
  - Body: “Here is that document you asked for… don’t show anyone else”

- When executed the macro automatically sent the email to 50 people in address book
  - Required MS Outlook to be running
  - Look like you receive an email from someone you know
  - It infects all other documents created on the computer

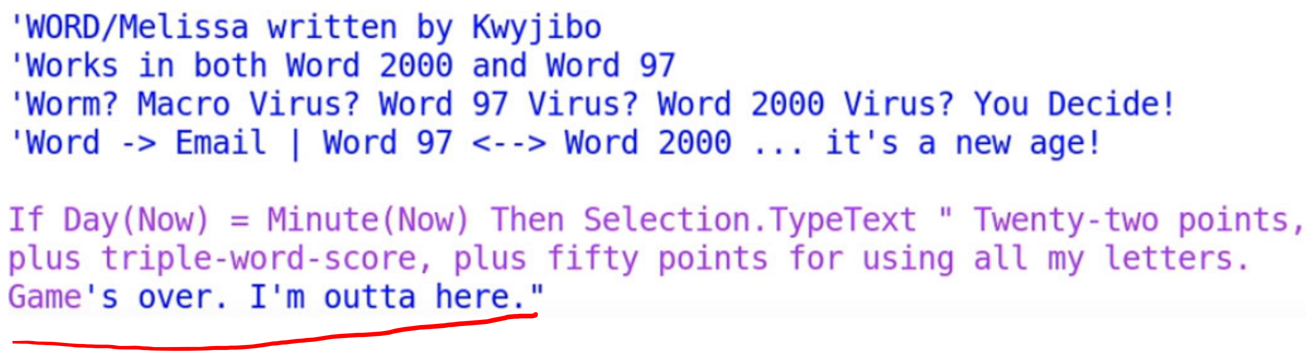
Macro-Virus (Melissa)

- Smith said: I had no idea that the virus would have this sort of impact and inflict this kind of damage. It was intended to be nothing more than a harmless joke.”

[illegible]

- Smith arrested in 1 April 1999. Mr. Smith went to the prison for 20 months, fined $5,000 and ordered, on release, to “not be involved with computer networks or internet unless authorized by the court”.

Macro-Virus (Melissa)



```
'WORD/Melissa written by Kwyjibo
'Works in both Word 2000 and Word 97
'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!

If Day(Now) = Minute(Now) Then Selection.TypeText " Twenty-two points,
plus triple-word-score, plus fifty points for using all my letters.
Game's over. I'm outta here."
```

Video Summary

- What is a Virus?
- Nature of Viruses
- Compression Virus
- Virus Classifications
- Macro-virus (Melissa)