# Malware

## Chapter Five – Part 2


By : Eman Talib Jasim

Department of Information Technology 2018-2019

# Outlines

- Virus Structure
- Virus Classifications
- Virus Types
- Anti Virus Evolution
- Anti Virus Approaches

# Virus Structure

```
    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:

}
```

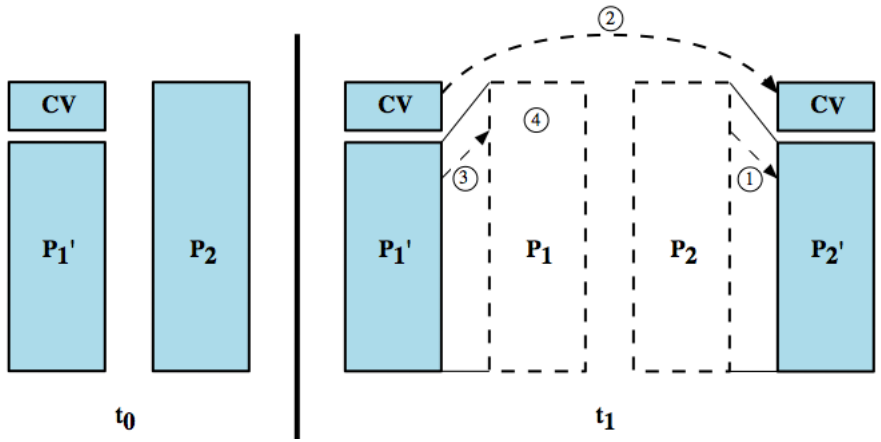
# Compression Virus

```
    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 Classification

- Parasitic virus

  - traditional and still most common form of virus.

  - attaches itsel to executable files and replicates .

- Memory-residence virus

  - lodges in main memory as part of resident system program

  - infects every program executes.

- boot sector virus

  - infects a master boot record and spreads when a system is booted from the disk containing the virus .

# Virus Classification Contin...

- Stealth virus

  - A form of virus explicitly designed to hide itself from detection by antivirus software .

- Polymorphic virus

  - a virus that mutates with every infection, making detection by signature impossible .

- Metamorphic virus

  - mutates with every infection

  - rewrite itself completely at each infection

  - may change their behavior as well as their appearance .

# Macro Virus

- became very common in mid-1990s since
  - platform independent
  - infect documents
  - easily spread
- exploit macro capability of office apps
  - executable program embedded in office doc
  - often a form of Basic
- more recent releases include protection
- recognized by many anti-virus programs

# E-Mail Viruses

- more recent development
- e.g. Melissa
  - exploits MS Word macro in attached doc
  - if attachment opened, macro activates
  - sends email to all on users address list
  - and does local damage
- then saw versions triggered reading email
- hence much faster propagation

# Virus Countermeasures

- prevention - ideal solution but difficult
- realistically need:
  - detection
  - identification
  - removal
- if detect but can't identify or remove, must discard and replace infected program

# Anti-Virus Evolution

- virus & antivirus tech have both evolved
- early viruses simple code, easily removed
- as become more complex, so must the countermeasures
- generations
  - first - signature scanners
  - second - heuristics
  - third - identify actions
  - fourth - combination packages

# Two main types

- there are different types of antivirus software for different computers
- some are designed for personal computers
- some are for servers and others for enterprises
- there are mainly two types of antivirus software:

  - specific scanning

  - generic scanning

# Specific Scanning

- specific scanning or signature detection
- the application scans files to look for known viruses matching definitions in a “virus dictionary”
- when the antivirus looks at a file it refers to a dictionary of known viruses and matches a piece of code (specific patterns of bytes) from the new file to the dictionary.

# Specific scanning cont..

- after recognizing the malicious software the antivirus software can take one of the following actions:
- (1): attempt to repair the file by removing the virus itself from the file
- (2): quarantine the file
- (3): or delete the file completely

# Specific scanning cont..

- however, specific scanning is not always reliable because virus authors are creating new ways of disguising their viruses so the antivirus software does not match the virus' signature to the virus dictionary.

# Generic Scanning

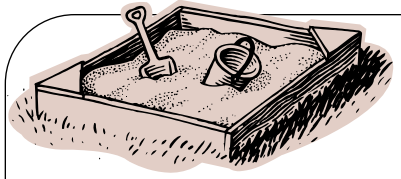
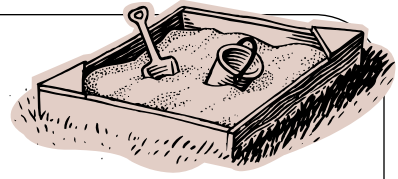
- generic scanning is also referred to as the suspicious behavior approach.
- generic Scanning is used when new viruses appear.
- in this method the software does not look for a specific signature but instead monitors the behavior of all applications.
- if anything questionable is found by the software the application is quarantined and a warning is broadcasted to the user about what the program may be trying to do.

# Generic Scanning cont...

- if the software is found to be a virus the user can send it to a virus vendor.
- there, researchers examine it, determine its signature, name and catalogue it and release antivirus software to stop its spread.
- if the virus never reappears the vendors categorize the virus as dormant.

# Two other approaches

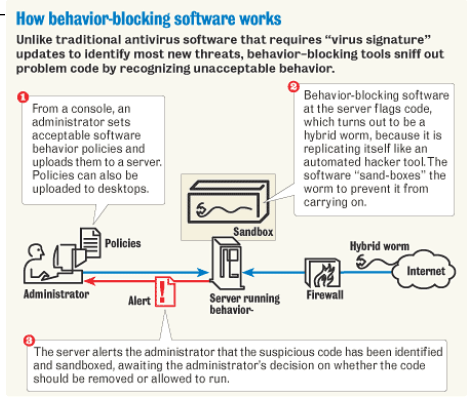
- heuristic analysis
  - another form of generic scanning
- the sandbox method

# Another Approach...

- heuristic analysis
  - this approach does not rely on a specific signature.
  - it looks for fragments of code that are often associated with viruses.
  - for example: a scanner may look for the beginning of an encryption loop used in a polymorphic virus to discover the encryption key.
  - once the key is discovered, the scanner can decrypt the virus to identify it .
  - finally remove the infection and return the program to service .

# Sandboxing




- in this approach an antivirus program will take suspicious code and run it in a "virtual machine" to see the purpose of the code and exactly how the code works.
- after the program is terminated the software analyzes the sandbox for any changes, which might indicate a virus.

# Advanced Anti-Virus Techniques

- Generic Decryption
- Digital Immune System
- Behavior – Blocking Software