CS 556 – Computer Security
Fall 2013

Dr. Indrajit Ray
Email: indrajit@cs.colostate.edu

Department of Computer Science
Colorado State University
Fort Collins, CO 80523, USA

MALWARE

Malware Terminology

- Virus – program that attaches itself to a host program and propagates copies of itself to other programs
- Worm – program that propagates copies of itself to other computers
- Logic bomb – program that triggers action when a particular condition occurs
- Trojan horse – program that hides itself in a host program and contains unexpected additional functionality
- Backdoor – program modification that allows unauthorized access to functionality
- Mobile code – software that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics

Malware Terminology

- Auto-rooter – malicious hacker tools used to break into new machines remotely
- Kit (virus generator) – set of tools for generating new viruses automatically
- Spammer and Flooder – programs that are used to send large volumes of unwanted e-mail, or to attack systems with a large volumes of traffic to carry out a DoS attack
- Keyloggers – programs that capture keystrokes on a compromised system
- Rootkit – set of hacker tools used after attacker has broken into a computer system and gained root-level access
- Zombie – program on infected machine activated to launch attacks on other machines

Viruses

- Piece of software that infects programs
  - Modifying them to include a copy of the virus
  - So it executes secretly when host program is run
- Specific to operating system and hardware
- Take advantage of their details and weaknesses
- A typical virus cycles through 4 phases in its lifecycle

Virus Phases

- **Dormant phase**: The virus is idle. The virus will eventually be activated by some event,
  - A date
  - The presence of another program or file
  - The capacity of the disk exceeding some limit.
- **Propagation phase**: The virus places an identical copy of itself into other programs or into certain system areas on the disk. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.
  - A virus will typically not propagate to another infected program

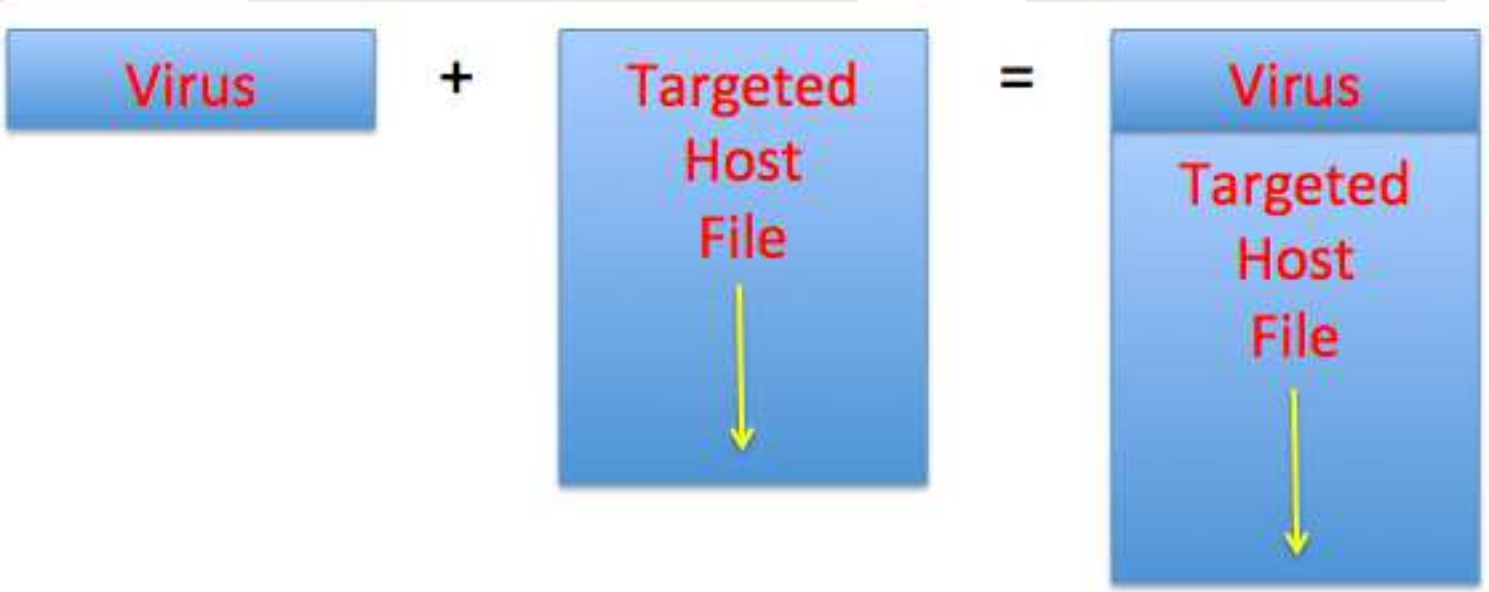
Virus Phases (continued)

- **Triggering phase**: The virus is activated to perform the function for which it was intended. Can be caused by a variety of system events
- **Execution phase**: The goal of the virus software is performed
  - Harmless - e.g. display message on screen
  - Malevolent - e.g. deletion of program or data files

Virus Structure

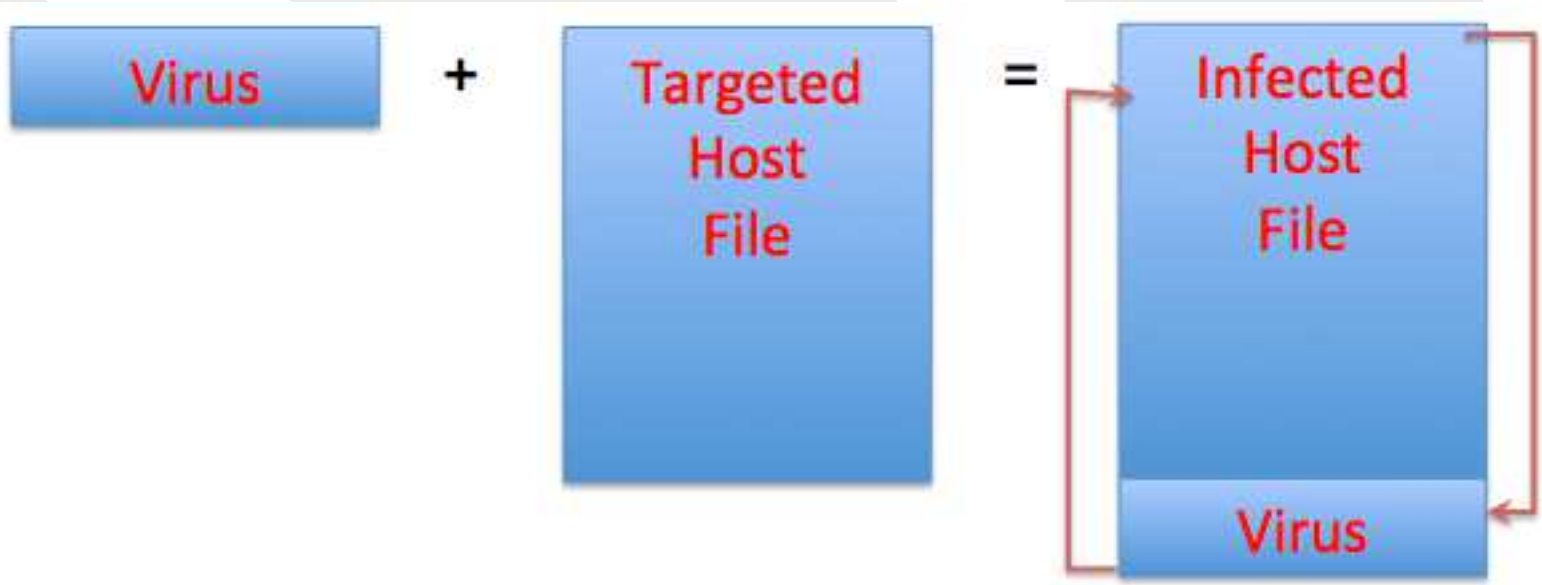

```
    program V :=

{goto main;
    1234567;                    <-- Virus DNA

    subroutine infect-executable :=
        {loop:
        file := get-random-executable-file;
        if (first-line-of-file = 1234567)
          then goto loop
          else prepend V to file; }          } Infection module

    subroutine do-damage :=
        {whatever damage is to be done}      } Payload

    subroutine trigger-pulled :=
        {return true if some condition holds} } Trigger

main:   main-program :=
        {infect-executable;
        if trigger-pulled then do-damage;
        goto next;}

next:

}
```

Virus Infection Model – Prepended



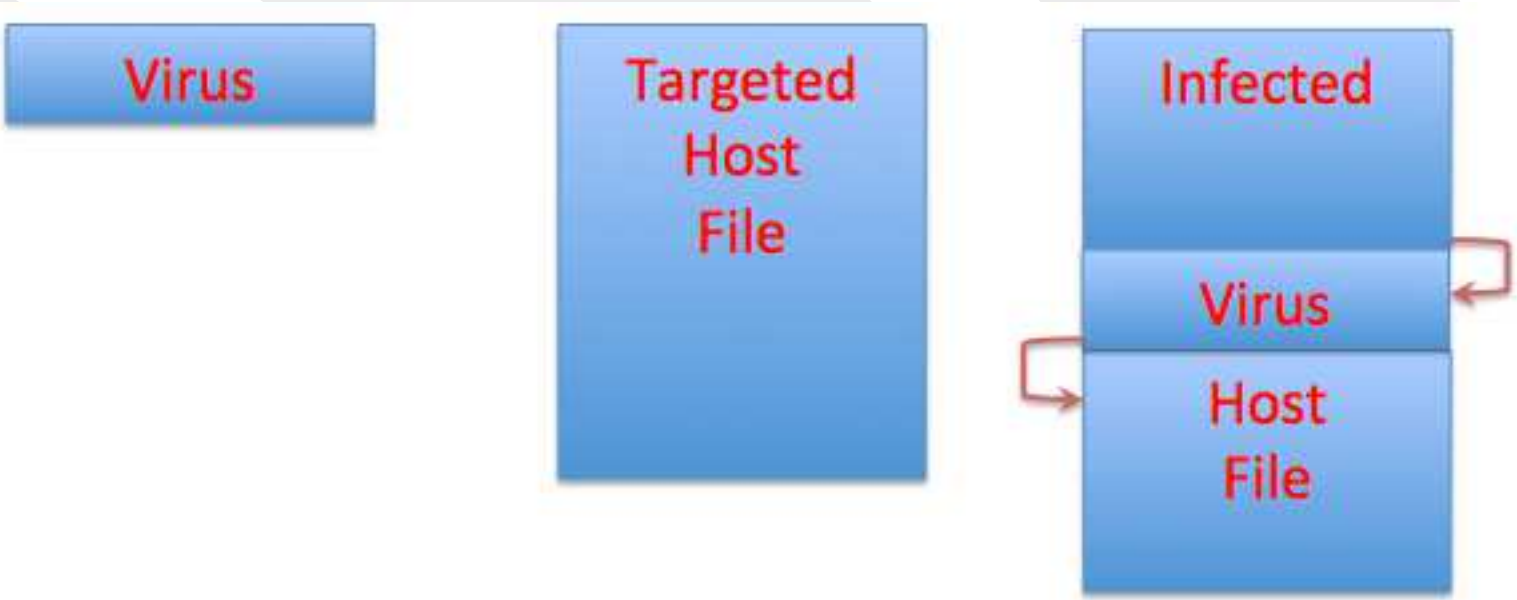
Does not damage the host program
Easier to clean

Virus Infection Model – Appended



Does not damage the host program
But more difficult to clean

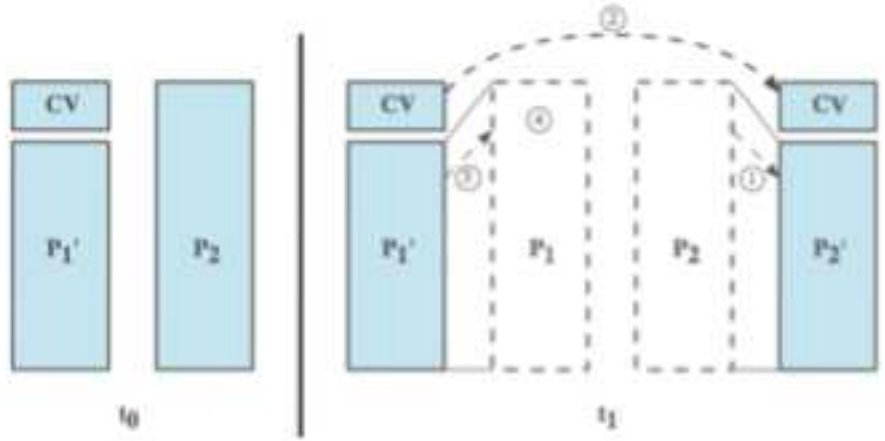
Virus Infection Model – Embedded



Damages the host program
Difficult to clean

Virus Infection Model – Compression


```
    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 (By Target)

- **Boot sector** – Infects a master boot record or partition 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 consider to be executable
- **Macro virus** – Infects files with macro code that is interpreted by an application

Virus Classification (By Concealment Strategy)

- **Encrypted Virus**
  - The virus creates a random encryption key, stores in the virus body, and encrypts the remainder of the virus.
  - When an infected program is invoked, the virus uses the stored random key to decrypt the virus.
  - When the virus replicates, a different random key is selected.

Virus Classification (By Concealment Strategy)

- **Stealth Virus**
  - Virus explicitly designed to hide itself from detection by antivirus software. Thus, the entire virus, not just a payload is hidden.
  - Hiding strategies
    - Intercept an antiviruss attempt to read a file (to detect virus) and presents a clean version of the file.
    - Slow down the infection rate
    - Set the hidden file attribute

Virus Classification (By Concealment Strategy)

- **Polymorphic Virus**
  - A virus that mutates with every infection, making detection by the "signature" of the virus virtually impossible
  - Mutation strategies
    - Change order in which instructions are included in the body of the virus
    - Introduce new instructions that do not do anything useful
    - Use encryption

Virus Classification (By Concealment Strategy)

- **Metamorphic Virus**
  - A metamorphic virus mutates with every infection.
    - Virus rewrites itself completely at each iteration, increasing the difficulty of detection.
    - Some even have the ability to dynamically disassemble themselves, change their code, and reassemble themselves into an executable form.
    - May change their behavior as well as their appearance in every incarnation.

Worms

- Replicating program that propagates over the network using email, remote exec, remote login
- Unlike a virus, does not require a host to propagate
- Has phases like a virus:
  - Dormant, propagation, triggering, execution
  - Propagation phase: searches for other systems, connects to it, copies self to it and runs
- May disguise itself as a system process

Worm Architecture

- A typical worm program has 5 components
  - Warhead
  - Propagation engine
  - Target selection algorithm
  - Scanning engine
  - Payload

Worm Warhead

- Code that exploits some vulnerability to break into a target system
- Most popular techniques
  - Buffer overflow attacks
  - File-sharing attacks
  - Email systems allowing executable attachments
  - Common misconfiguration most notably use of default password

Propagation Engine

- Warhead opens the door to the target system. The Propagation Engine transfers the rest of the body of the worm into the system
- Most popular propagation protocols
  - File Trasfer Protocol (FTP - uses clear-text user-id and password)
  - Trivial File Transfer Protocol (TFTP allows unauthenticated access)
  - Hyper Text Trasfer Protocol (HTTP)
  - Server Message Block protocol (SMB - used for Windows file sharing. Unix servers running SAMBA support SMB)

Target Selection

- Looks for new victims to attack
- Most popular techniques
  - Email addresses
  - Host lists (from /etc/hosts or LMHOSTS)
  - Trusted systems (from .rhosts or equivalent files)
  - Network neighborhood (using NetBIOS or SMB protocol)
  - DNS Queries
  - Randomly selecting target network address

Scanning Engine

- Scans the network for suitable victim using the list of targets generated by the target selection engine
- Popular techniques
  - Open ports scanning
  - Vulnerability scanning

Worm Payload

- Code designed to implement some specific action on the target system
  - Plant a backdoor, spammer, keylogger, rootkit etc.
  - Plant a DDoS flood Agent (to allow launching a DDoS attack remotely)
  - Perform complex mathematical operation (typically cracking crypto keys)

Recent Advances in Worm Technology

- **Multiplatform**: Newer worms are not limited to specific OS, but can attack a variety of platforms, especially the popular varieties of UNIX.
- **Multi-exploit**: Newer worms penetrate systems in a variety of ways, using exploits against Web servers, browsers, email, file-sharing, and other network based applications
- **Ultrafast spreading**: Instead of scanning in real time, include list of target machines in worm body
- **Polymorphic**: Each copy of the worm has new code generated on the fly using functionally equivalent instructions and encryption techniques.
- **Metamorphic**: The worm has a repertoire of behavior patterns that are unleashed at different stages of propagation