

Lecture Outline

- Malware
 - terminology
- Viruses
- Worms



© Madartists

Adapted from Computer Security: Principles and Practice, Stallings and Lawrie

Taxonomy

Terminology

- Virus
 - fragments of code attaches itself to a program and propagates copies of itself to other programs
- Worm
 - program that propagates copies of itself to other computers on the network
- Logic bomb
 - program which lies dormant until a predefined condition is met – it then triggers an unauthorized act
- Trojan horse
 - apparently useful or innocuous application with hidden malicious software
- Backdoor (trapdoor)
 - secret entryway into a program (advantages?)
- Keyloggers
 - captures key strokes on a compromised system
- Zombie, bot
 - program on an infected machine that is activated to launch attacks on other machines
- Spyware
 - software that collects information from a comp. and transmits to another sys.
- Adware
 - advertising that is integrated into software – can result in pop-up ads or redirection to a targeted site

Backdoors

Viruses

- A virus has 3 parts
 1. Infection mechanism/ infection vector: the means via which it spreads and replicates
 2. Trigger: the event or condition that determines when the payload is activated or triggered/ delivered
 3. Payload: the “havoc” the virus is designed to create

Viruses

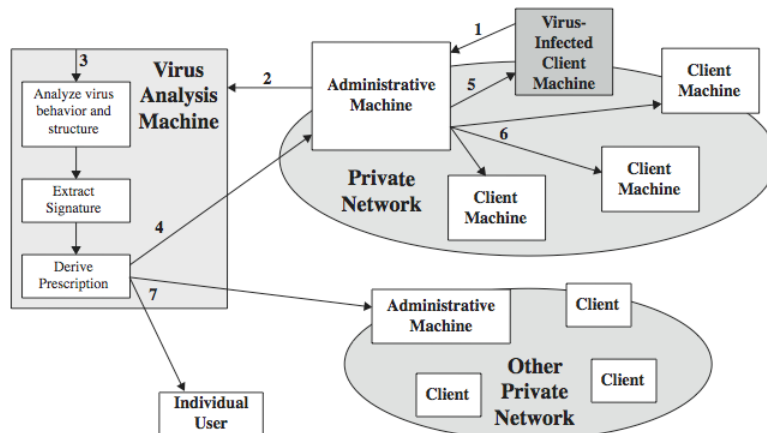
- A virus goes through 4 main phases
 1. **Dormant:** idle – waiting for event such as date, presence or absence of another file/ program
 2. **Propagation:** virus places a copy of itself into other programs, these in turn place copies into other programs etc.
 3. **Triggering:** the event is triggered
 4. **Execution:** the havoc is carried out (e.g. deleting files) – can also be harmless as pop-up boxes

Anti-Virus Evolution

- Advances in virus and anti-virus technology go hand in hand
- A **first-generation** scanner requires a **virus signature to identify a virus**. Such signature-specific scanners are limited to the detection of known viruses.
- A **second-generation** scanner uses **heuristic rules to search for probable virus infection**, e.g to look for fragments of code that are often associated with viruses.
- Third-generation** programs are memory-resident programs that **identify a virus by its actions** rather than structure in an infected program. These have the advantage that it is not necessary to develop signatures / heuristics, but only to identify the small set of actions indicating an infection is attempted and then intervene.
- Fourth-generation** products are packages consisting of a **variety of antivirus techniques used in conjunction**. These include scanning and activity trap components.

Digital Immune System

- comprehensive approach to virus protection, developed by IBM (97) and refined by Symantec (01)



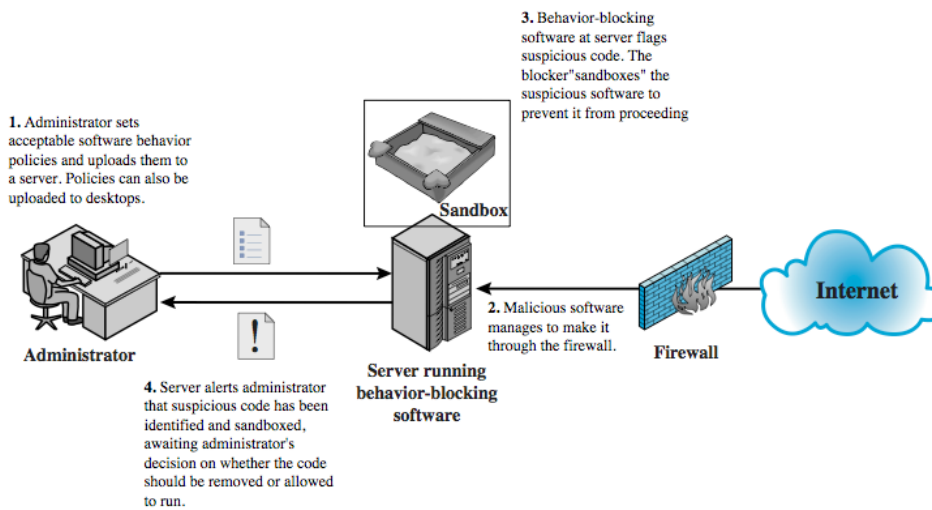
Digital Immune System (Heuristic)

1. A monitoring program on each PC uses a variety of **heuristics** to infer that a virus may be present, and forwards a copy to an administrative machine
2. The admin machine encrypts this and sends it to a central virus analysis machine
3. This machine creates an environment in which the infected program can be safely run for analysis. The virus analysis machine then produces a prescription for identifying and removing the virus
4. The resulting prescription is sent back to the administrative machine
5. The administrative machine forwards the prescription to the infected client
6. The prescription is also forwarded to other clients in the organization
7. Subscribers worldwide receive regular antivirus updates to protect from new virus

The success of the digital immune system depends on the ability of the virus analysis machine to detect new and innovative virus strains. By constantly analyzing and monitoring the viruses found in the wild, it should be possible to continually update the digital immune software to keep up with the threat.

Behavior-Blocking Software Operations

- Unlike heuristics or fingerprint-based scanners, behavior-blocking software integrates with the operating system of a host computer and monitors program behavior in real-time for malicious actions.



Behavior-Blocking Software Operations

The behavior blocking software blocks potentially malicious actions before they can affect the system. Monitored behaviors can include:

Attempts to open, view, delete, and/or modify files;

Modifications to executable files or macros;

Modification of critical system settings, such as start-up settings;

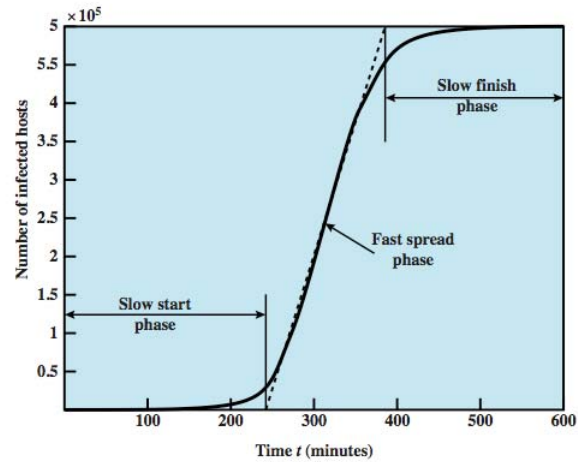
Scripting of e-mail and instant messaging clients to send executable content;

Initiation (frequent and/ or unexpected) of network communications

Worms

- replicating program that propagates over net
 - using email, remote exec, remote login
- 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 Propagation Model



CSCI 415: Computer and Network Security

Dr. Nazli Hardy

Adapted from Computer Security: Principles and Practice, Stallings and Lawrie

Worm Countermeasures

- overlaps with anti-virus techniques
- once worm on system anti-virus can usually detect
- worms additionally cause significant net activity
- worm defense approaches include:
 - signature-based worm scan filtering
 - generates a **worm signature**, which is then used to prevent worm scans from entering/leaving a network/host
 - filter-based worm containment
 - focuses on **worm content** rather than a scan signature. The filter checks a message to determine if it contains **worm code**
 - payload-classification-based worm containment
 - **examine packets** to see if they contain a worm using anomaly detection techniques

CSCI 415: Computer and Network Security

Dr. Nazli Hardy

Adapted from Computer Security: Principles and Practice, Stallings and Lawrie

