جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

قسم الامن السيبراني
Department of Cyber Security

Subject:

Malicious codes

Class:

THIRD

Lecturer:

Dr. Suha Alhussieny

Lecture: (3)

Multiple-Threat Malware , Viruses

Multiple-Threat Malware

In modern cybersecurity, malware has evolved from simple viruses to complex, multi-functional threats. Traditional malware was usually designed to exploit one method of infection. For example, a classic virus infected only executable files, while a worm spread mainly through networks. However, attackers soon realized that combining multiple techniques makes malware more powerful, harder to detect, and faster to spread.

- **Multiple-threat malware** is malware that operates in more than one way, using different infection or distribution strategies.
- It does not rely on a single vulnerability or method but instead mixes several methods to increase damage and survivability.

Two major categories we discuss are:

1. Multipartite Viruses
2. Blended Attacks

Multipartite Viruses

A multipartite virus is a type of virus that can infect different types of files or areas of a system at the same time.

Characteristics

- Can infect both executable files and boot sectors.
- Harder to remove, because even if one infection site is cleaned, another may reinfect the system.

- Requires comprehensive antivirus scanning to identify all infection points.

Example

- The Tequila virus (early 1990s) was able to infect both program files and the boot sector of a disk.

Impact

- Increases persistence of infection.
- Makes eradication more complex.

Blended Attacks

A blended attack combines multiple methods of infection and multiple malware types in one coordinated attack package.
It is not just one virus or one worm—it may include viruses, worms, Trojans, and exploits together.

Goals

- Maximize speed of spread.
- Increase severity of damage.
- Exploit many vulnerabilities at once.

Techniques Used

- Email attachments (social engineering).
- File sharing systems (unprotected network shares).
- Exploiting web servers (vulnerabilities in server software).

- Web-based drive-by infections (malicious code injected into websites).

Case Study: The Nimda Attack (2001)

The Nimda malware is a famous blended attack.

- Often mistakenly described as just a worm, but in reality, Nimda used four different distribution methods simultaneously.

Distribution Methods

1. E-mail
    - Spread through infected email attachments.
    - Scanned for email addresses on a victim's system and sent itself automatically.
2. Windows Shares
    - Searched for open/unsecured file shares in Windows.
    - Used the NetBIOS protocol to copy itself across the network.
3. Web Servers
    - Scanned for vulnerabilities in Microsoft IIS (Internet Information Services).
    - Uploaded itself to vulnerable servers, infecting both the server and its files.
4. Web Clients

- If a user visited a Nimda-infected website with a vulnerable browser, the workstation would become infected automatically.

Consequences

- Nimda spread extremely quickly worldwide.
- Damaged both enterprise systems and individual users.
- Highlighted the need for defense-in-depth strategies.

Security measures

1. Defense-in-depth is essential

   Firewalls, antivirus, intrusion detection, and secure configurations must work together.

2. User awareness

   Users must recognize phishing attempts, suspicious attachments, and unsafe downloads.

3. Network monitoring

   Malware that spreads across shares and servers can often be detected by unusual traffic patterns.

Computer Viruses

- A **computer virus** is one of the oldest and most well-known forms of malware.
- The name comes from **biological viruses** because they behave in a similar way:

- They insert themselves into a host.
- They replicate and spread to new hosts.
- They can cause harmful or disruptive effects.

❖ Computer viruses first appeared in the **early 1980s** and quickly became a major cybersecurity concern.

What is a Computer Virus?

- A **virus** is a piece of software that can **infect other programs** by modifying them.
- The modification usually includes **inserting the virus code** into the program.
- When the infected program is executed, the virus code also runs, allowing it to spread.

Analogy to Biology

- Biological viruses use **DNA/RNA** to hijack a cell and make copies of themselves.
- Similarly, computer viruses carry code that makes copies of themselves in other programs or files.

How Viruses Spread

- Viruses spread by **infecting executable programs** and then moving to other computers.
- Early methods of spreading:

- **Floppy disks** (users unknowingly shared infected programs).

- Modern methods:
  - **Networks and the Internet** (email attachments, file sharing, downloads).
- Networks provide a **perfect culture for viral spread**, since users and systems constantly exchange files and services.

What Can a Virus Do?

- A virus can do **anything any other program can do** (depending on user privileges).
- Typical actions:
  - **Harmless:** displaying a message or an image.
  - **Harmful:** deleting files, corrupting data, or disabling system functions.

Structure of a Virus

A computer virus has **three essential parts**:

1. **Infection Mechanism (Vector):**
   - The method the virus uses to spread and replicate.
   - Examples: attaching to files, boot sectors, macros.
2. **Trigger:**
   - The condition that activates the virus payload.

- Examples: a specific date, a certain number of executions, or detection of a file.

3. **Payload:**
   - The actual function of the virus, aside from replication.
   - Can be **benign** (pranks, messages) or **malicious** (data deletion, system corruption).

Lifecycle of a Virus

A typical virus goes through **four phases** during its life:

1. **Dormant Phase:**
   - Virus is inactive, waiting for a condition (e.g., a date, disk usage limit).
   - Not all viruses have this phase.
2. **Propagation Phase:**
   - Virus replicates itself by infecting other files or areas of the disk.
   - Sometimes modifies its code to **evade detection** (polymorphic viruses).
3. **Triggering Phase:**
   - Some event activates the payload.
   - Example: virus triggers on April 1st or after 100 replications.
4. **Execution Phase:**

- The payload is executed.
- Can be harmless (a joke message) or harmful (file deletion, ransomware).

Initial Infection

- A virus begins by infecting **a single program**.
- Once that program runs, the virus can spread to other files and the system.
- Prevention must focus on **blocking the virus from entering the system**.

Modern Situation

- Traditional **machine-code viruses** are less common today.
- Modern systems face new types of malware (worms, Trojans, ransomware).
- Still, the **concept of viruses** is crucial to understanding the evolution of malware.

Security measure

1. **Prevent entry:** control what software enters your system.
2. **Use access controls:** limit user privileges to reduce spread.
3. **Patch systems regularly:** many viruses exploit outdated software.
4. **User awareness:** never open unknown attachments or files.
5. **Antivirus and monitoring tools:** detect and stop virus activity.

H.W1/ Discussion Questions

1. Why is it harder to remove a multipartite virus compared to a normal virus?
2. How does Nimda demonstrate the concept of a blended attack?
3. What defense strategies would you recommend to prevent such attacks today?
4. Can you think of modern malware examples that use blended attack techniques?

H.W2/

1. Which of the following best describes multiple-threat malware?
2. A multipartite virus can infect:
3. Which early virus was able to infect both program files and the boot sector?
4. Why are multipartite viruses harder to remove?
5. A blended attack usually includes:
6. The Nimda malware (2001) is an example of:
7. Which of the following was NOT a Nimda distribution method?
8. Nimda spread quickly worldwide because it:
9. Defense-in-depth strategy includes:
10. Which security practice helps reduce malware infections?
11. A computer virus is named after biological viruses because:
12. The infection mechanism of a virus refers to:
13. Which virus component activates the payload?
14. Which virus component is the actual malicious or benign action?
15. Which is NOT part of the virus lifecycle?
16. In the dormant phase, a virus is:
17. Which virus phase involves replicating and spreading?

18. A virus payload can be:
19. Which was an early method of virus spreading?
20. A modern virus is less likely to spread through:
21. Which is a recommended security measure?
22. What is the first step in virus infection?
23. Which part of a virus lifecycle may not always exist?
24. Viruses that change their code to evade detection are called:
25. Why are computer viruses still studied today?