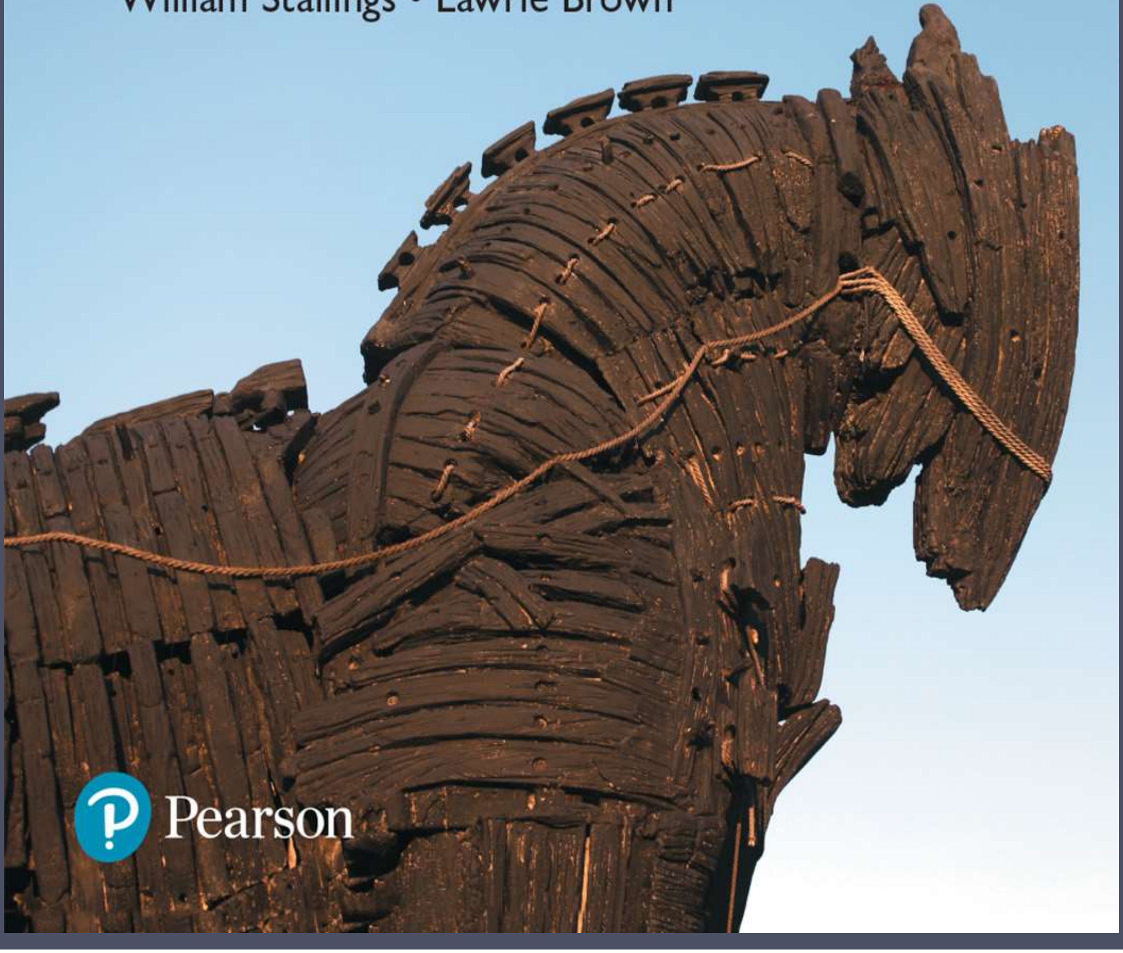
GLOBAL
EDITION

Computer Security

Principles and Practice

FOURTH EDITION

William Stallings • Lawrie Brown



Pearson

Chapter 5

Malicious Software and Attacks

Malicious software, or malware

Malicious software, or **malware**, arguably constitutes one of the most significant categories of threats to computer systems.

Malware can be defined as

"A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim."

Types of Malicious Software (Malware)

Name	Description
Advanced Persistent Threat (APT)	Cybercrime directed at business and political targets, using a wide variety of intrusion technologies and malware, applied persistently and effectively to specific targets over an extended period, often attributed to state-sponsored organizations.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.
Attack kit	Set of tools for generating new malware automatically using a variety of supplied propagation and payload mechanisms.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Backdoor (trapdoor)	Any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality in a program, or onto a compromised system.
Downloaders	Code that installs other items on a machine that is under attack. It is normally included in the malware code first inserted on to a compromised system to then import a larger malware package.

Types of Malicious Software (Malware)

Name	Description
Flooders (DoS client)	Used to generate a large volume of data to attack networked computer systems, by carrying out some form of denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Logic bomb	Code inserted into malware by an intruder. A logic bomb lies dormant until a predefined condition is met; the code then triggers an unauthorized act.
Macro virus	A type of virus that uses macro or scripting code, typically embedded in a document, and triggered when the document is viewed or edited, to run and replicate itself into other such documents.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.
Spammer programs	Used to send large volumes of unwanted e-mail.

Types of Malicious Software (Malware)

Name	Description
Spyware	Software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data, and/or network traffic; or by scanning files on the system for sensitive information.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes it.
Virus	Malware that, when executed, tries to replicate itself into other executable machine or script code; when it succeeds, the code is said to be infected. When the infected code is executed, the virus also executes.
Worm	A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network, by exploiting software vulnerabilities in the target system, , or using captured authorization credentials.
Zombie, bot	Program installed on an infected machine that is activated to launch attacks on other machines.

Components of Computer Virus

A computer virus has three parts. More generally, many contemporary types of malware also include one or more variants of each of these components:

- **Infection mechanism**: The means by which a virus spreads or propagates, enabling it to replicate. The mechanism is also referred to as the **infection vector**.
- **Trigger**: The event or condition that determines when the payload is activated or delivered, sometimes known as a **logic bomb**.
- **Payload**: What the virus does, besides spreading. The payload may involve damage or may involve benign but noticeable activity.

Phases of Computer Virus lifetime

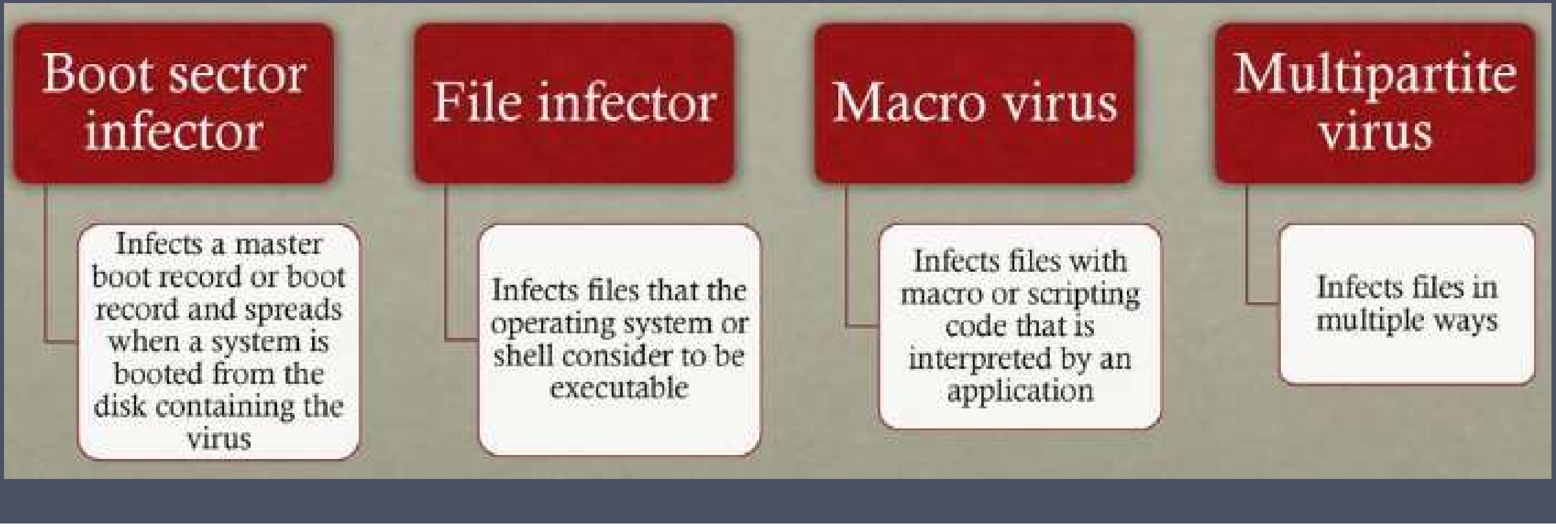
During its lifetime, a typical virus goes through the following four phases:

1. **Dormant phase**: The virus is idle. The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit. Not all viruses have this stage.
2. **Propagation phase**: The virus places a copy of itself into other programs or into certain system areas on the disk.
3. **Triggering phase**: The virus is activated to perform the function for which it was intended.
4. **Execution phase**: The function is performed. The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.

Virus Classification (based on target)

A virus classification by **target** includes the following categories:

1. **Boot sector infector**: Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.
2. **File infector**: Infects files that the operating system or shell consider to be executable.
3. **Macro virus**: Infects files with macro or scripting code that is interpreted by an application.
4. **Multipartite virus**: Infects files in multiple ways. Typically, the multipartite virus is capable of infecting multiple types of files, so that virus eradication must deal with all of the possible sites of infection.


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 consider 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

Viruses Classification

(based on concealment strategy)

A virus classification by concealment strategy includes the following categories:

1. **Encrypted virus**: A form of virus that uses encryption to obscure it's content. A portion of the virus creates a random encryption key and encrypts the remainder of the virus. The key is stored with the virus. When an infected program is invoked, the virus uses the stored random key to decrypt the virus.
2. **Stealth virus**: A form of virus explicitly designed to hide itself from detection by anti-virus software. Thus, the entire virus, not just a payload is hidden. It may use code mutation, compression, or rootkit techniques to achieve this.

Viruses Classification

(based on concealment strategy)

3. **Polymorphic virus**: A form of virus that creates copies during replication that are functionally equivalent but have distinctly different bit patterns, in order to defeat programs that scan for viruses. In this case, the "signature" of the virus will vary with each copy.
4. **Metamorphic virus**: As with a polymorphic virus, a metamorphic virus mutates with every infection. The difference is that a metamorphic virus rewrites Itself completely at each iteration, using multiple transformation techniques, increasing the difficulty of detection. Metamorphic viruses may change their behavior as well as their appearance.

Phishing and Identity Theft

- An approach used to capture a user’s login and password credentials is to include a URL in a spam e-mail that links to a fake Web site controlled by the attacker, but which mimics the login page of some banking, gaming, or similar site.
- This is normally included in some message suggesting that urgent action is required by the user to authenticate their account, to prevent it being locked.
- This is known as a **phishing** attack and exploits social engineering to leverage user’s trust by masquerading as communications from a trusted source

Spear-phishing

A more dangerous variant of phishing is the **spear-phishing** attack. This again is an e-mail claiming to be from a trusted source. However, the recipients are carefully researched by the attacker, and each e-mail is carefully crafted to suit its recipient specifically, often quoting a range of information to convince them of its authenticity.

This greatly increases the likelihood of the recipient responding as desired by the attacker.

Malware Countermeasure Approaches

Prevention Approach

The ideal solution to the threat of malware is prevention: Do not allow malware to get into the system in the first place, or block the ability of it to modify the system. This goal is, in general, nearly impossible to achieve, although taking suitable countermeasures to harden systems and users in preventing infection can significantly reduce the number of successful malware attacks. .

- **Updating:** One of the first countermeasures that should be employed is to ensure all systems are as current as possible, with all patches applied, in order to reduce the number of vulnerabilities that might be exploited on the system.
- **Access Control:** The next is to set appropriate access controls on the applications and data stored on the system, to reduce the number of files that any user can access, and hence potentially infect or corrupt, as a result of them executing some malware code.
- **User Awareness:** The third common propagation mechanism, which targets users in a social engineering attack, can be countered using appropriate user awareness and training.

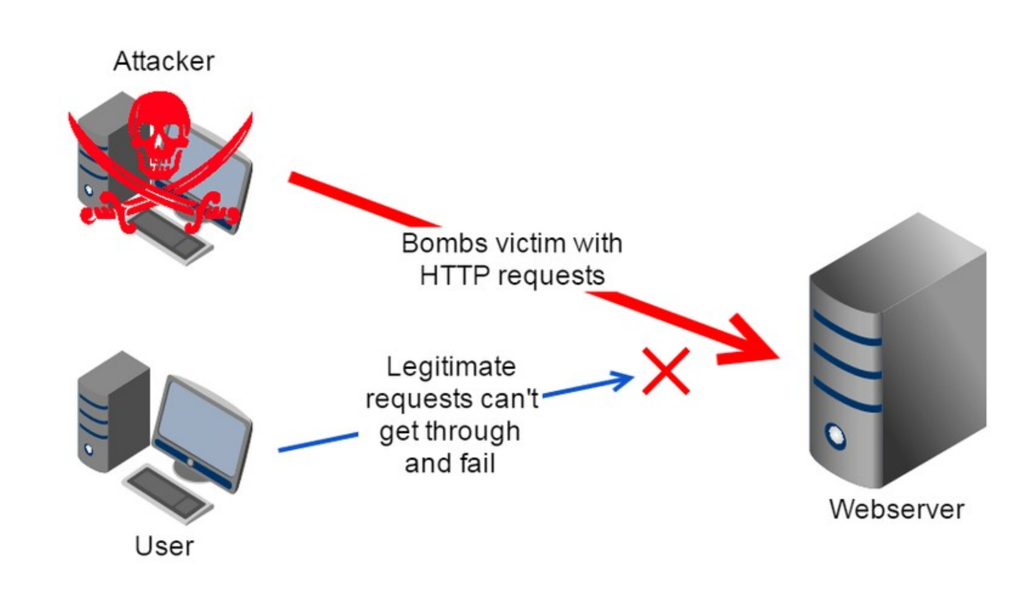
Malware Countermeasure Approaches

If **prevention fails**, then technical mechanisms can be used to support the following threat mitigation options:

- **Detection:** Once the infection has occurred, determine that it has occurred and locate the malware.
- **Identification**: Once detection has been achieved, identify the specific malware that has infected the system.
- **Removal**: Once the specific malware has been identified, remove all traces of malware virus from all infected systems so that it cannot spread further.

Denial-of-Service (DoS) attack

"A denial of service (DoS) is an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space."


Attacker
Bombs victim with HTTP requests
Legitimate requests can't get through and fail
Webserver
User

Forms of DoS attack

- A form of attack on the availability of some service
- Categories of resources that could be attacked are:

Network bandwidth

Relates to the capacity of the network links connecting a server to the Internet

For most organizations this is their connection to their Internet Service Provider (ISP)

System resources

Aims to overload or crash the network handling software

Application resources

Typically involves a number of valid requests, each of which consumes significant resources, thus limiting the ability of the server to respond to requests from other users

Distributed Denial of Service (DDoS) Attacks

Use of multiple systems to generate attacks

Attacker uses a flaw in operating system or in a common application to gain access and installs their program on it (zombie)

Large collections of such systems under the control of one attacker's control can be created, forming a botnet

Defenses against denial-of-service Attacks

- There are a number of steps that can be taken both to limit the consequences of being the target of a DoS attack and to limit the chance of your systems being compromised and then used to launch DoS attacks.
- In a **distributed denial-of-service attack** (**DDoS attack**), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.
- The defense against DoS and DDoS attacks have been discussed in next slide.

Defense against DoS or DDoS attacks

In general, there are four lines of defense against DoS or DDoS attacks:

1. **Attack prevention and preemption (before the attack)**: These mechanisms enable the victim to endure attack attempts without denying service to legitimate clients.
2. **Attack detection and filtering (during the attack)**: These mechanisms attempt to detect the attack as it begins and respond immediately. This minimizes the impact of the attack on the target.
3. **Attack source traceback and identification (during and after the attack)**: This is an attempt to identify the source of the attack as a first step in preventing future attacks.
4. **Attack reaction (after the attack)**: This is an attempt to eliminate or curtail the effects of an attack.

Thank You!