UNIVERSITY OF WESTMINSTER

Malicious Software

6COSC019W- Cyber Security

Dr Ayman El Hajjar

February 20, 2024

School of Computer Science and Engineering
University of Westminster

Outline

Malicious Software

MALWARE

NIST 800-83 defines malware 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.

NCSC defines malware as:

"a term that includes virus, trojans, worms or any code or content that could have an adverse impact on organisations or individuals..

Malicious Code and Activity

- Any program that carries out actions that you (user/System) did not intend to do is considered to be a Malicious software (malware)
- Malicious code attacks one or more of the three information security properties:
  - **Confidentiality**: Malware can disclose your organisation's private information
  - **Integrity**: Malware can modify database records, either immediately or over a period of time
  - **Availability**: Malware can erase or overwrite files or inflict considerable damage to storage media

Characteristics, Architecture, and Operations of Malicious Software

- An attacker gains administrative control of a system and uses commands to inflict harm
- An attacker sends commands directly to a system; the system interprets and executes them
- An attacker uses software programs that harm a system or that make the data unusable
- An attacker uses legitimate remote administration tools and security probes to identify and exploit security vulnerabilities on a network

Malware Classifications

MALWARE CLASSIFICATION APPROACH

- The original approach to classify malware focuses on how they spread or propagate through an information system environment to reach the desired target/s
- A more conventional approach was developed to consider all dimensions of malware in order to classify them.
- This approach is used by the NCSC and it contains the following dimensions:
  - Host dependent or independent
  - persistent or transient
  - Where it install itself (persistent malware only)
  - How it is triggered
  - Static or dynamically updated
  - Act alone or coordinated attack

MALWARE CLASSIFICATION APPROACH

- Host dependent or Independent malware
  - **Independent malware or standalone** is a complete program that can run on its own once it is installed on a compromised machine and executed.
  - **Host dependent malware** requires a host program to run. It cannot run independently, but infect a program on a computer by inserting its instructions into the program or modifying the host code.
- Persistent or Transient
  - **Persistent malware** are installed in persistent storage such as a file system (your hard drive) or an external storage device. They can be either standalone or host independent.
  - **Transient malware** are installed in volatile memory such as as RAM memory.

MALWARE CLASSIFICATION APPROACH

- Where it install itself
  - This dimension generally applies to only persistent malware (Ones that requires installation)
  - Malware are categorised based on which layer of the system stack the malware is installed and run on
  - this could the firmware, the boot sector, the operating system level, the driver, the api, or user application
- How it is triggered
  - **Auto-spreading malware** runs and then looks for other vulnerable machines on the Internet, compromises these machines and installs itself on them;
  - **User-activated malware** is run on a computer only because a user accidentally downloads and executes it, e.g., by clicking on an attachment or URL in a received email.

MALWARE CLASSIFICATION APPROACH

- Static or dynamically updated
  - Malware that are supported by an infrastructure and can still communicate with such infrastructure are dynamically updated with new version regularly.
  - Static malware or one time malware has no infrastructure to support it and are standalone software with no network connection to an external infrastructure
- Act alone or coordinated attack
  - **Act alone malware** are isolated malware that runs on their own. They do not participate in a larger scale attack. Such malware usually have a specific target.
  - **Coordinated malware** are attacks that contribute to a larger scale attack as on their own they will not cause much damage. For example, collectively several devices infected by such malware can cause networks or systems to crash (DDoS).

Malware Types

MALWARE CONTENTS

- Malware are divided into two parts:
  - Infection mechanism: How it propagates
  - The Payload: what happens after it reaches the target

Propagation mechanisms include:

- Infection of existing content by viruses that is subsequently spread to other systems
- Exploit of software vulnerabilities by worms or drive-by-downloads to allow the malware to replicate
- Social engineering attacks that convince users to bypass security mechanisms to install Trojans or to respond to phishing attacks

Payload actions performed by malware once it reaches a target system can include:

- Corruption of system or data files
- Theft of service/make the system a zombie agent of attack as part of a botnet
- Theft of information from the system/keylogging
- Stealthing/hiding its presence on the system

The Main Types of Malware

- Virus
- Spam
- Worms
- Trojan horses
- Logic bombs
- Active content vulnerabilities
- Malicious add-ons
- Botnets
- Denial of service attacks
- Spyware
- Adware
- Phishing
- Keystroke loggers
- Hoaxes and myths
- Homepage hijacking
- Webpage defacements

VIRUS

- Piece of software that infects programs
  - Modifies them to include a copy of the virus
  - Replicates and goes on to infect other content
  - Easily spread through network environments
- When attached to an executable program a virus can do anything that the program is permitted to do
  - Executes secretly when the host program is run
- Specific to operating system and hardware
  - Takes advantage of their details and weaknesses

VIRUS COMPONENTS

Infection Mechanism

- Means by which a virus spreads or propagates
- Also referred to as the infection vector

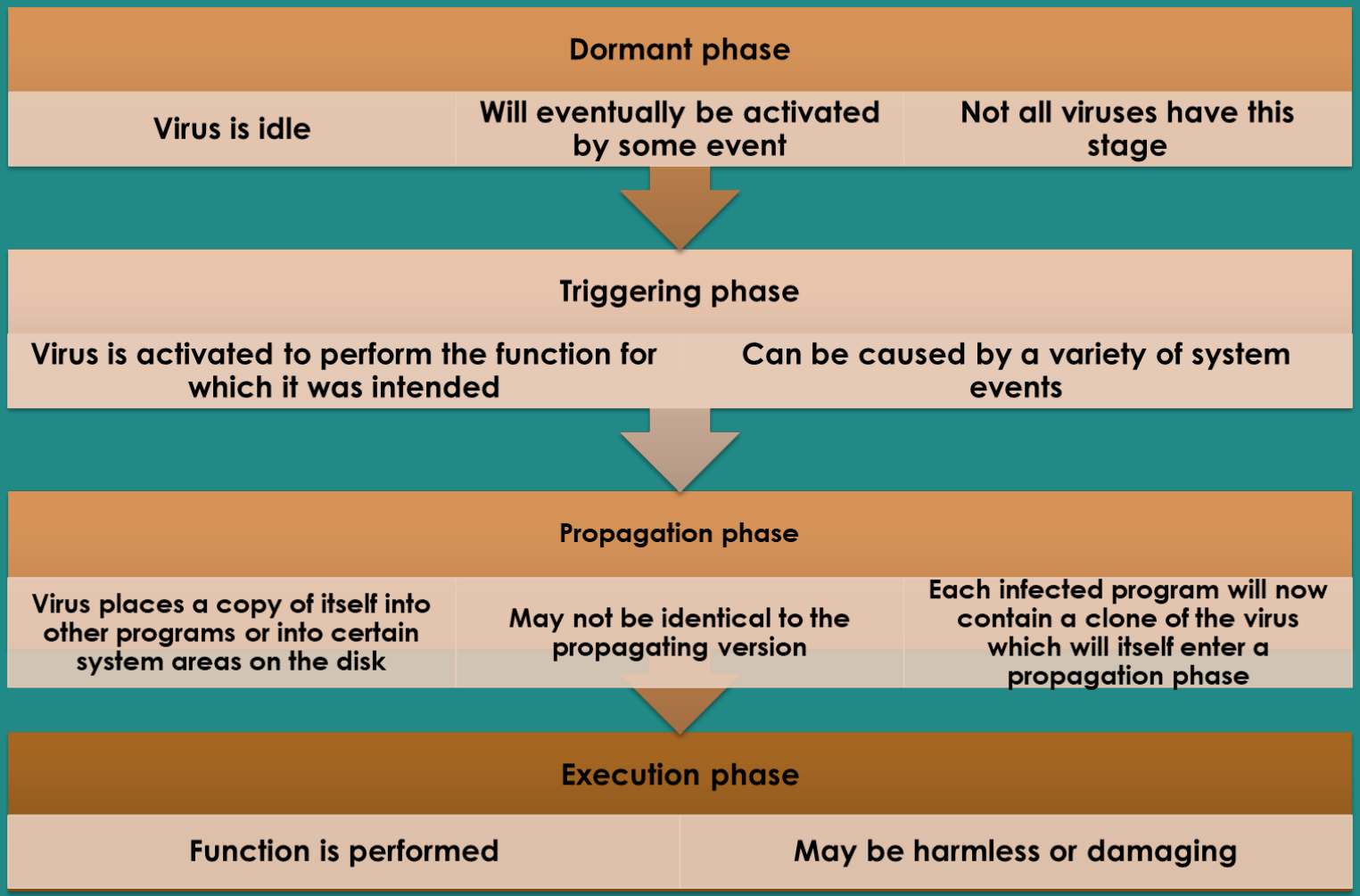
Trigger

- 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)
- May involve damage or benign but noticeable activity

VIRUS PHASES



Virus Classifications: By Targets

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 Infectors

- Infects files that the operating system or shell considers 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

VIRUS CLASSIFICATIONS: BY CONCEALMENT STRATEGY

Encrypted virus

- A portion of the virus creates a random encryption key and encrypts the remainder of the virus

Stealth virus

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

Polymorphic virus

- A virus that mutates with every infection

Metamorphic virus

- A virus that mutates and rewrites itself completely at each iteration and may change behaviour as well as appearance

MALVERTISING

- Places malware on websites without actually compromising them
- The attacker pays for advertisements that are highly likely to be placed on their intended target websites and incorporate malware in them
- Using these malicious ads, attackers can infect visitors to sites displaying them
- The malware code may be dynamically generated to either reduce the chance of detection or to only infect specific systems
- Has grown rapidly in recent years because they are easy to place on desired websites with few questions asked and are hard to track
- Attackers can place these ads for as little as a few hours, when they expect their intended victims could be browsing the targeted websites, greatly reducing their visibility

CLICKJACKING

- Also known as a user-interface (UI) redress attack
- Using a similar technique, keystrokes can also be hijacked
  - A user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker
- Vulnerability used by an attacker to collect an infected user's clicks
  - The attacker can force the user to do a variety of things from adjusting the user's computer settings to unwittingly sending the user to Web sites that might have malicious code
  - A typical attack uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page
  - The attacker is hijacking clicks meant for one page and routing them to another page

Social Engineering

- "Tricking" users to assist in the compromise of their own systems

Spam

- Unsolicited bulk e-mail
- Significant carrier of malware
- Used for phishing attacks

Trojan horse

- Program or utility containing harmful hidden code
- Used to accomplish functions that the attacker could not accomplish directly

Mobile phone Trojans

- First appeared in 2004 (Skuller)
- Target is the smartphone

MACRO AND SCRIPTING VIRUS

- Macro virus infect scripting code used to support active content in a variety of user document types
- Are threatening for a number of reasons:
  - Is platform independent
  - Infect documents, not executable portions of code
  - Are easily spread
  - Because they infect user documents rather than system programs, traditional file system access controls are of limited use in preventing their spread, since users are expected to modify them
  - Are much easier to write or to modify than traditional executable virus

MACRO AND SCRIPTING VIRUS: TRUSTED DOWNLOAD?

ACTIVE CONTENT VIRUS

- Active content
  - Refers to dynamic objects that do something when the user opens a webpage (ActiveX, Java, JavaScript, VBScript, macros, browser plugins, PDF files, and other scripting languages)
  - Has potential weaknesses that malware can exploit
- Active content threats are considered mobile code because these programs run on a wide variety of computer platforms
- Users download bits of mobile code, which gain access to the hard disk and do things like fill up desktop with infected file icons

WORMS

- Program that actively seeks out more machines to infect and each infected machine serves as an automated launching pad for attacks on other machines
- Exploits software vulnerabilities in client or server programs
- Usually carries some form of payload

Electronic mail or instant messenger facility	• Worm e-mails a copy of itself to other systems • Sends itself as an attachment via an instant message service
File sharing	• Creates a copy of itself or infects a file as a virus on removable media
Remote execution capability	• Worm executes a copy of itself on another system
Remote file access or transfer capability	• Worm uses a remote file access or transfer service to copy itself from one system to the other
Remote login capability	• Worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other

WORM TECHNOLOGY

1. **Multiplatform**: Worms are not Operating System specific.
2. **Multi-exploit**: Worms penetrate systems using a variety of methods
3. **Ultrafast spreading**: Exploit various techniques to optimize the rate of spread of the worm
4. **Polymorphic**: To evade detection, skip past filters, and foil real-time analysis, worms adopt the virus polymorphic technique.
5. **Metamorphic**: In addition to changing their appearance, metamorphic worms have a collection of behaviour patterns that are unleashed at different stages of propagation.
6. **Zero-day exploit** : To achieve maximum surprise and distribution, a worm should exploit an unknown vulnerability that is only discovered by the general network community when the worm is launched.

ROOTKITS

- Type of malware that modifies or replaces one or more existing programs to hide the fact that a computer has been compromised
- Modify parts of the operating system to conceal traces of their presence
- Provide attackers with access to compromised computers and easy access to launching additional attacks
- Difficult to detect and remove

ROOTKITS CLASSIFICATION CHARACTERISTICS

1. **Persistent**: Activates each time the system boots. The rootkit must store code in a persistent store, such as the registry or file system, and configure a method by which the code executes without user intervention.
2. **Memory based:** Has no persistent code and therefore cannot survive a reboot. However, because it is only in memory, it can be harder to detect.
3. **User mode**: Intercepts calls to APIs (application program interfaces) and modifies returned results.
4. **Kernel mode**: Can intercept calls to native APIs in kernel mode. The rootkit can also hide the presence of a malware process by removing it from the kernel's list of active processes.
5. **External mode:** The malware is located outside the normal operation mode of the targeted system, in BIOS or system management mode, where it can directly access hardware.

Payload Classifications

PAYLOAD

- Payload are classified based on the damage or threat they bring to the system
- The different classes of payload are:
  - System Corruption
  - Attack Agents Bots
  - Remote Control Facility
  - Information Theft- Keyloggers and Spyware
  - Information Theft- Phishing
  - Stealthing Backdoor
  - Stealthing Rootkit

System Corruption

- Causes damage to physical equipment such as Stuxnet worm
  - Targets specific industrial control system software
- There are concerns about using sophisticated targeted malware for industrial sabotage

PAYLOAD CLASSES

Attack Agents Bots

- Takes over another Internet attached computer and uses that computer to launch or manage attacks
- Botnet collection of bots capable of acting in a coordinated manner
  - For example DDoS botnets

Remote Control Facility

- Typical means of implementing the remote control facility is on an IRC server
  - Bots join a specific channel on this server and treat incoming messages as commands

PAYLOAD CLASSES

Information Theft- Keyloggers and Spyware

- Keyloggers
  - Captures keystrokes to allow attacker to monitor sensitive information
- Spyware
  - Subverts the compromised machine to allow monitoring of a wide range of activity on the system

Information Theft- Phishing

- Phishing exploits social engineering to leverage the user's trust by masquerading as communication from a trusted source
  - Include a URL in a spam e-mail that links to a fake Web site that mimics the login page of a banking, gaming, or similar site
  - Attacker exploits the account using the captured credentials

PAYLOAD CLASSES

Stealthing Backdoor

- Secret entry point into a program allowing the attacker to gain access and bypass the security access procedures
- Also called a trapdoor , used by maintenance as well as malicious actors
- Difficult to implement operating system controls for backdoors in applications

Stealthing Rootkit

- Set of hidden programs installed on a system to maintain covert access to that system
- Gives administrator (or root) privileges to attacker
  - Can add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand

Threats & Countermeasures

MALWARE COUNTERMEASURE APPROACHES

- Ideal solution to the threat of malware is prevention

Four main elements of prevention

- Policy
- Awareness
- Vulnerability mitigation
- Threat mitigation

- If prevention fails, technical mechanisms can be used to support the following threat mitigation options:
  - Detection
  - Identification
  - Removal

GENERATIONS OF ANTI-VIRUS SOFTWARE

First generation: simple scanners

- Requires a malware signature to identify the malware
- Limited to the detection of known malware

Second generation: heuristic scanners

- Uses heuristic rules to search for probable malware instances
- Another approach is integrity checking

Third generation: activity traps

- Memory-resident programs that identify malware by its actions rather than its structure in an infected program

Fourth generation: full-featured protection

- Packages consisting of a variety of anti-virus techniques used in conjunction
- Include scanning and activity trap components and access control capability

REFERENCES

- The lecture notes and contents were compiled from my own notes and from various sources.
- Figures and tables are from the recommended books
- **The lecture notes are very detailed. If you attend the lecture, you should be able to understand the topics.**
- **You can use any of the recommended readings! You do not need to read all the chapters!**
- **Recommended Readings note:** Focus on what was covered in the class.
  - Chapter 8, Malware, CEH v11 Certified Ethical Hacker Study Guide
  - Chapter 8, Malicious Software and Attack Vectors, Fundamentals of Information Systems Security
  - Chapter 6, Malware and attack Technologies, CyBOK, The Cyber Security Body of Knowledge