UNIVERSITY OF
WESTMINSTER

Malicious Software

6COSC019W- Cyber Security

Dr Ayman El Hajjar

February 27, 2023

School of Computer Science and Engineering
University of Westminster

Outline

1. Malicious Software
2. Malware Taxonomy
3. Malware Types
4. Payload Classifications
5. Threats & Countermeasures

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 viruses, 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 organization'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

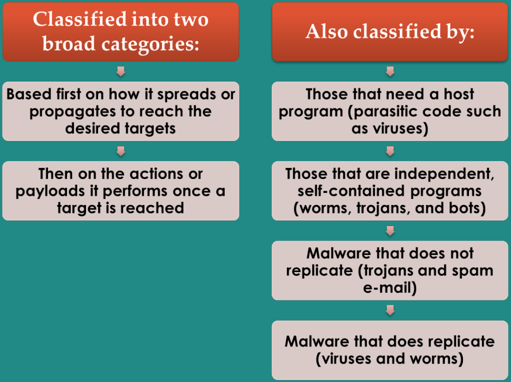
Characteristics, Architecture, and Operations of Malicious Software

- ✺ 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 Taxonomy

Malware Classification approaches

- The original approach to classify malware focuses on how they spread or propagate through an information system environment to reach the desired target/s
- Other approaches considered further how they infect, the purpose, how they are triggered, etc..



Classified into two broad categories:

Based first on how it spreads or propagates to reach the desired targets

Then on the actions or payloads it performs once a target is reached

Also classified by:

Those that need a host program (parasitic code such as viruses)

Those that are independent, self-contained programs (worms, trojans, and bots)

Malware that does not replicate (trojans and spam e-mail)

Malware that does replicate (viruses and worms)

MALWARE TAXONOMY

- 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 TAXONOMY

- 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.

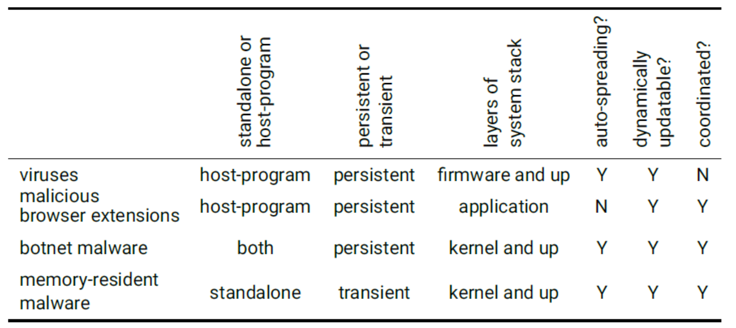
MALWARE TAXONOMY

- 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 TAXONOMY

- 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 CLASSIFICATION EXAMPLES

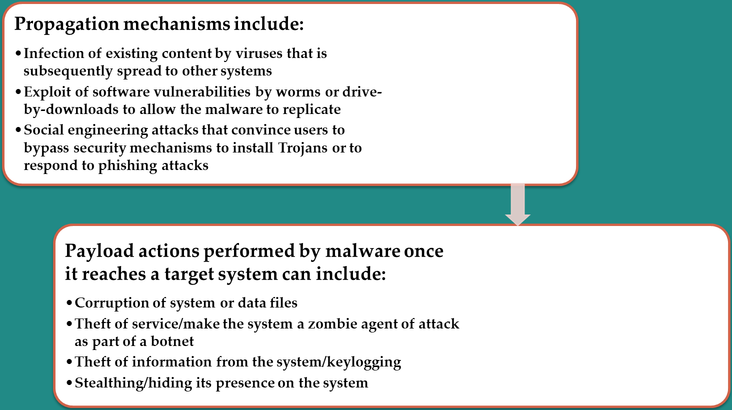


	standalone or host-program	persistent or transient	layers of system stack	auto-spreading?	dynamically updatable?	coordinated?
viruses	host-program	persistent	firmware and up	Y	Y	N
malicious browser extensions	host-program	persistent	application	N	Y	Y
botnet malware	both	persistent	kernel and up	Y	Y	Y
memory-resident malware	standalone	transient	kernel and up	Y	Y	Y

Use of the Taxonomy to Classify Representative Malware. CyBOK, chapter 6, table 6.1

Malware Types

Malware Types



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

- Viruses
- 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

ATTACK KITS

- Initially the development and deployment of malware required considerable technical skill by software authors
- The development of virus-creation toolkits in the early 1990s and then more general attack kits in the 2000s greatly assisted in the development and deployment of malware
- Toolkits are often known as “crimeware”
  - Include a variety of propagation mechanisms and payload modules that even novices can deploy
  - Variants that can be generated by attackers using these toolkits creates a significant problem for those defending systems against them
- Example of attack kits are Zeus and Angler

Attack Sources

- Another significant malware development is the change from attackers being individuals often motivated to demonstrate their technical competence to their peers to more organized and dangerous attack sources such as:

Politically motivated attackers

Criminals

Organized crime

Organizations that sell their services to companies and nations

National government agencies

- This has significantly changed the resources available and motivation behind the rise of malware and has led to development of a large underground economy involving the sale of attack kits, access to compromised hosts, and to stolen information

Advanced Persistent Threats (APTs)

- ✺ Well-resourced, persistent application of a wide variety of intrusion technologies and malware to selected targets (usually business or political)
- ✺ Typically attributed to state-sponsored organizations and criminal enterprises
- ✺ Differ from other types of attack by their careful target selection and stealthy intrusion efforts over extended periods
- ✺ High profile attacks include Aurora, RSA, APT1, and Stuxnet

APT CHARACTERISTICS

Advanced

✺ Used by the attackers of a wide variety of intrusion technologies and malware including the development of custom malware if required

Persistent

✺ Determined application of the attacks over an extended period against the chosen target

✺ A variety of attacks may be progressively applied until the target is compromised

Threats

✺ Threats to the selected targets intent to compromise the specifically chosen targets

✺The active involvement of highly skilled, well financially and politically supported people in the process raises the threat level

APT Attacks

Aims

- ✺ Varies from theft of intellectual property or security and infrastructure related data to the physical disruption of infrastructure

Techniques used

- ✺ It could be something as simple as Social engineering, Spear-phishing email
- ✺ or as sophisticated that requires specially designed attack vectors

Intent

- ✺ To infect the target with sophisticated malware with multiple propagation mechanisms and payloads
- ✺ Once they have gained initial access to systems in the target organization a further range of attack tools are used to maintain and extend their access

VIRUSES

- 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

VIRUSES COMPONENTS

Infection Mechanism

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

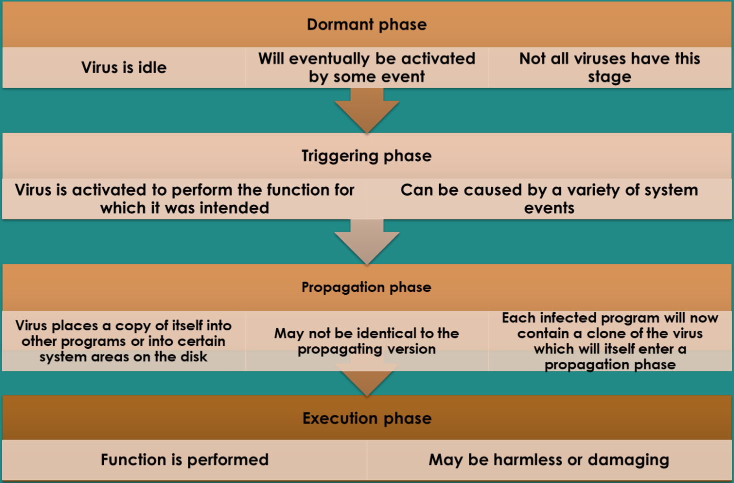
Trigger

- ✺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

Viruses Phases



Dormant phase

- Virus is idle
- Will eventually be activated by some event
- Not all viruses have this stage

Triggering phase

- Virus is activated to perform the function for which it was intended
- Can be caused by a variety of system events

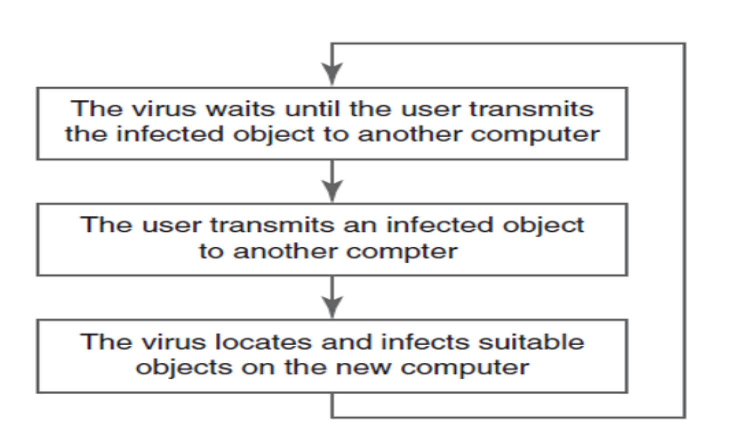
Propagation phase

- Virus places a copy of itself into other programs or into certain system areas on the disk
- May not be identical to the propagating version
- Each infected program will now contain a clone of the virus which will itself enter a propagation phase

Execution phase

- Function is performed
- May be harmless or damaging

TYPICAL LIFE CYCLE OF A COMPUTER VIRUS



The virus waits until the user transmits the infected object to another computer

The user transmits an infected object to another compter

The virus locates and infects suitable objects on the new computer

PROROGATION PHASE: TARGET DISCOVERY

- Scanning (or fingerprinting)
  - Network worm: Searches for other systems to infect
- Random
  - Each compromised host probes random addresses in the IP address space potentially causing disruption even before the actual attack is launched
- Hit-list
  - The attacker infects a long list of potential vulnerable machines and infects them. Each infected machine is provided scan a portion of the list
- Topological
  - This method uses information contained on an infected victim machine to find more hosts to scan
- Local subnet
  - The host uses the subnet address structure to find other hosts that would otherwise be protected by the firewall

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 behavior as well as appearance

DRIVE BY DOWNLOADS ATTACKS

- ✺ Exploits browser and plugin vulnerabilities so when the user views a webpage controlled by the attacker, it contains code that exploits the bug to download and install malware on the system without the user’s knowledge or consent
- ✺ In most cases the malware does not actively propagate as a worm does
- ✺ Spreads when users visit the malicious Web page

Watering-Hole Attacks

- A variant of drive-by-download used in highly targeted attacks
- The attacker researches their intended victims to identify websites they are likely to visit, then scans these sites to identify those with vulnerabilities that allow their compromise
- They then wait for one of their intended victims to visit one of the compromised sites
- Attack code may even be written so that it will only infect systems belonging to the target organization and take no action for other visitors to the site
- This greatly increases the likelihood of the site compromise remaining undetected

MALVERTISING

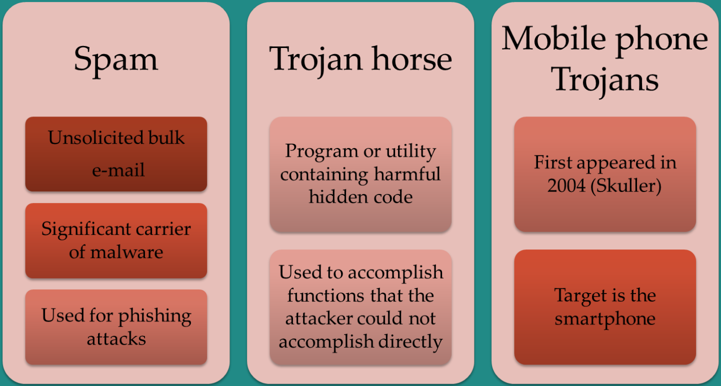
- Places malware on websites without actually compromising them
- The attacker pays for advertisements that are highly likely to be placed on their intended target websites and incorporate malware in them
- Using these malicious ads, attackers can infect visitors to sites displaying them
- The malware 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

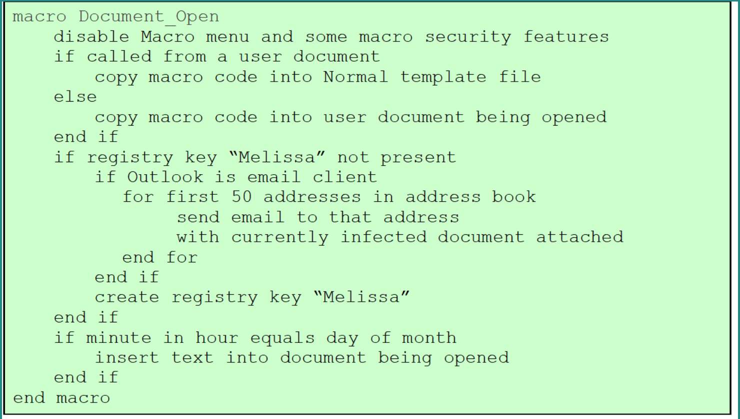
First appeared in 2004 (Skuller)

Target is the smartphone

Macro and Scripting viruses

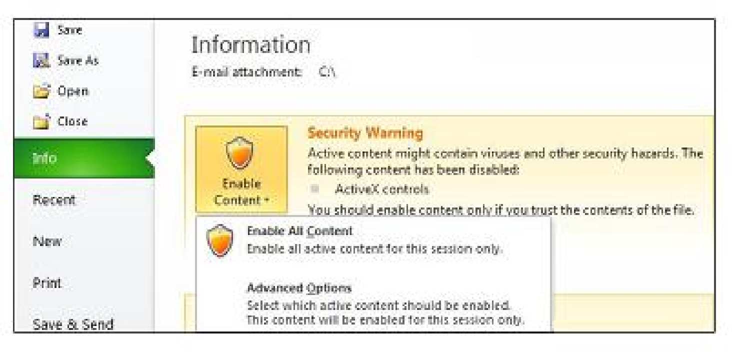
- Macro viruses infect scripting code used to support active content in a variety of user document types
- Are threatening for a number of reasons:
    - Is platform independent
    - Infect documents, not executable portions of code
    - Are easily spread
    - Because they infect user documents rather 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 viruses

MACRO AND SCRIPTING VIRUSES: PSEUDOCODE



```
macro Document_Open
    disable Macro menu and some macro security features
    if called from a user document
        copy macro code into Normal template file
    else
        copy macro code into user document being opened
    end if
    if registry key “Melissa” not present
        if Outlook is email client
          for first 50 addresses in address book
               send email to that address
               with currently infected document attached
          end for
        end if
        create registry key “Melissa”
    end if
    if minute in hour equals day of month
        insert text into document being opened
    end if
end macro
```

Macro and Scripting viruses: Trusted Download?



Information

E-mail attachment: C:\

Security Warning

Active content might contain viruses and other security hazards. The following content has been disabled:

- ActiveX controls

You should enable content only if you trust the contents of the file.

Enable All Content

Enable all active content for this session only.

Advanced Options

Select which active content should be enabled. This content will be enabled for this session only.

ACTIVE CONTENT VIRUSES

- 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
- ✺ Can use network connections to spread from system to system
- ✺ Spreads through shared media (USB drives, CD, DVD data disks)
- ✺ E-mail worms spread in macro or script code included in attachments and instant messenger file transfers
- ✺ Upon activation the worm may replicate and propagate again
- ✺ Usually carries some form of payload
- ✺ First known implementation was done in Xerox Palo Alto Labs in the early 1980s

Worms Replication

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.

Ransomware: WannaCry

1. Infected a large number of systems in many countries in May 2017
2. When installed on infected systems, it encrypted a large number of files and then demanded a ransom payment in Bitcoins to recover them
3. Recovery of this information was generally only possible if the organization had good backups and an appropriate incident response and disaster recovery plan
4. Targets widened beyond personal computer systems to include mobile devices and Linux servers
5. Tactics such as threatening to publish sensitive personal information, or to permanently destroy the encryption key after a short period of time, are sometimes used to increase the pressure on the victim to pay up

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- SYSTEM CORRUPTION

1. Real-world damage
   - ✺Causes damage to physical equipment
     - ❍ Chernobyl virus rewrites BIOS code
   - ✺ Stuxnet worm
     - ☛ Targets specific industrial control system software
   - ✺ There are concerns about using sophisticated targeted malware for industrial sabotage
2. ✺ Logic bomb
   - ✺ Code embedded in the malware that is set to “explode” when certain conditions are met

PAYLOAD- 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
- Uses:
  - Distributed denial-of-service (DDoS) attacks
  - Spamming
  - Sniffing traffic
  - Keylogging
  - Spreading new malware
  - Installing advertisement add-ons and browser helper objects (BHOs)
  - Attacking IRC chat networks
  - Manipulating online polls/games

PAYLOAD- REMOTE CONTROL FACILITY

✺ Distinguishes a bot from a worm

- ❍ Worm propagates itself and activates itself
- ❍ Bot is initially controlled from some central 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
- ❍ More recent botnets use covert communication channels via protocols such as HTTP
- ❍ Distributed control mechanisms use peer-to-peer protocols to avoid a single point of failure

PAYLOAD- INFORMATION THEFT KEYLOGGERS AND SPYWARE

1. Keyloggers

   ✺ Captures keystrokes to allow attacker to monitor sensitive information

   ✺ Typically uses some form of filtering mechanism that only returns information close to keywords (“login”, “password”)

2. Spyware

   ✺ Subverts the compromised machine to allow monitoring of a wide range of activity on the system

   ❍ Monitoring history and content of browsing activity

   ❍ Redirecting certain Web page requests to fake sites

   ❍ Dynamically modifying data exchanged between the browser and certain Web sites of interest

PAYLOAD- INFORMATION THEFT PHISHING

1. 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

    ✺ Suggests that urgent action is required by the user to authenticate their account

    ✺ Attacker exploits the account using the captured credentials

2. Spear-phishing

    ✺ Recipients are carefully researched by the attacker

    ✺ E-mail is crafted to specifically suit its recipient, often quoting a range of information to convince them of its authenticity

PAYLOAD- STEALTHING BACKDOOR

- Also known as a trapdoor
- Secret entry point into a program allowing the attacker to gain access and bypass the security access procedures
- Maintenance hook is a backdoor used by Programmers to debug and test programs
- Difficult to implement operating system controls for backdoors in applications

Payload- Stealthing Rootkit

- Set of hidden programs installed on a system to maintain covert access to that system
- Hides by subverting the mechanisms that monitor and report on the processes, files, and registries on a computer
- 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

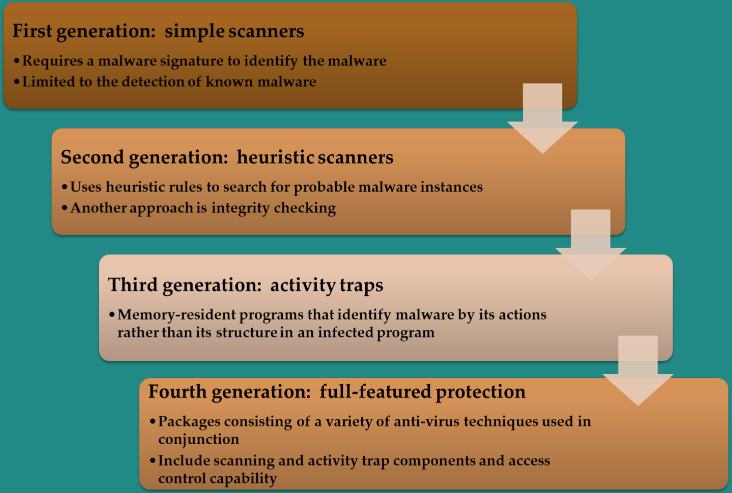
- Ideal solution to the threat of malware is prevention

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

SANDBOX ANALYSIS

- ✺ Running potentially malicious code in an emulated sandbox or on a virtual machine
- ✺ Allows the code to execute in a controlled environment where its behavior can be closely monitored without threatening the security of a real system
- ✺ Running potentially malicious software in such environments enables the detection of complex encrypted, polymorphic, or metamorphic malware
- ✺ The most difficult design issue with sandbox analysis is to determine how long to run each interpretation

Host-Based Behaviour-Blocking Software

- Integrates with the operating system of a host computer and monitors program behavior in real time for malicious action
  - Blocks potentially malicious actions before they have a chance to affect the system
  - Blocks software in real time so it has an advantage over anti-virus detection techniques such as fingerprinting or heuristics

Limitations

- Because malicious code must run on the target machine before all its behaviors can be identified, it can cause harm before it has been detected and blocked

PERIMETER SCANNING APPROACHES

✷ Anti-virus software typically included in e-mail and Web proxy services running on an organization's firewall and IDS

✷ Approach is limited to scanning malware

Two types of monitoring software

1. Ingress Monitors
   - ❍ Located at the border between the enterprise network and the Internet
   - ❍ One technique is to look for incoming traffic to unused local IP addresses
2. Egress monitors
   - ❍ Located at the egress point of individual LANs as well as at the border between the enterprise network and the Internet
   - ❍ Monitors outgoing traffic for signs of scanning or other suspicious behaviour

REFERENCES

- The lecture notes and contents were compiled from my own notes and from various sources.
- Figures and tables are from the recommended books
- **Recommended Readings note:** Focus on what was covered in the class.
  - Chapter 6, Computer Security: Principles and Practice, , William Stallings and Lawrie Brown
  - Chapter 6, CyBOK, The Cyber Security Body of Knowledge