Week 08:

Any program that carries out actions that you (user/System) did not intend to do is a Malicious software.

**Confidentiality**: Malware can disclose your organisation’s private information.

**Integrity**: Malware can modify database records, either immediately or over a period.

**Availability**: Malware can erase or overwrite files or infect considerable damage to storage media

Characteristics

* gains administrative control.
* sends commands directly to a system.
* attacker uses software programs.
* attacker uses legitimate remote administration tools.

**MALWARE CLASSIFICATION APPROACH**

**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.

**Persistent malwares** 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 malwares** are installed in volatile memory such as RAM memory.

**Where it installs itself**

❐ applies to only persistent malware (Ones that requires installation)

❐ categorised based on which layer of the system stack the malware is installed - This could be 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.

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 malware** are isolated malware that runs on their own. They do not participate in a larger scale attack. Such malware usually has 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 are divided into two parts:

* Infection mechanism: How it propagates
* The Payload: what happens after it reaches the target.

A screenshot of a computer

Description automatically generated !!!!!!!! Important

A computer screen shot of a computer

Description automatically generated

A virus is a piece of malicious software that attaches itself to other programs or files and infects them by modifying their code to include a copy of itself.

Viruses are often tailored to exploit vulnerabilities specific to certain operating systems and hardware configurations. They take advantage of these details and weaknesses to infiltrate and propagate.

**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.

A diagram of a virus

Description automatically generated

**VIRUS CLASSIFICATIONS: BY TARGETS**

**Boot sector infector** Infects a master 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 virus.

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

**Polymorphic virus** A virus that modifies 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**

The attacker pays for advertisements that are highly likely to be placed on their intended target websites and incorporate malware in them.

**CLICKJACKING**

known as a user-interface (UI) redress attack.

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.

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.

A diagram of a program

Description automatically generated with medium confidence

**MACRO AND SCRIPTING VIRUS**

Macro virus infect scripting code used to support active content in a variety of user document types.

Are threatening for several 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.

The type of virus that infects documents by executing active content once it is opened is called a "Macro" virus.

**ACTIVE CONTENT VIRUS**

Refers to dynamic objects within webpages or documents that perform actions when opened by users, including ActiveX, Java, JavaScript, VBScript, macros, browser plugins, PDF files, and other scripting languages.

Has potential weaknesses that malware can exploit.

Active content threats are categorized as mobile code because they execute on various computer platforms.

Users unknowingly download bits of mobile code, which can then gain access to the hard disk and perform malicious actions.

**WORMS**

Worms actively seek out and infect other machines, using each infected machine as a launchpad for further attacks.

exploit vulnerabilities in client or server programs, such as operating systems.

Worms typically carry payloads, which can include malicious code designed to disrupt systems, steal data, or create backdoors for remote access.

A group of text on a table

Description automatically generated with medium confidence

Multiplatform: Worms are not limited to specific operating systems,

Multi-exploit: Worms utilize various methods to penetrate systems, exploiting multiple vulnerabilities or weaknesses to gain unauthorized access.

Ultrafast Spreading: Employing various techniques, worms optimize their spread rate, enabling them to propagate rapidly across networks and infect numerous systems in a short amount of time.

Polymorphic: Worms employ polymorphic techniques similar to viruses, altering their code to escape detection by antivirus software, bypass filters, and thwart real-time analysis.

Metamorphic: In addition to changing their appearance, metamorphic worms exhibit a range of behaviour patterns during different stages of propagation, making them more challenging to detect and mitigate.

Zero-day Exploit: For maximum impact and distribution, worms may exploit unknown vulnerabilities, known as zero-day exploits. These vulnerabilities are typically not disclosed to the public until the worm is launched, maximizing the element of surprise and enabling widespread infection before patches or countermeasures can be developed.

**ROOTKITS**

Rootkits are a type of malware designed to modify or replace existing programs on a computer to conceal the fact that the system has been compromised.

They modify various parts of the operating system to hide traces of their presence.

Rootkits provide attackers with unauthorized access to compromised computers, allowing them to execute additional attacks or maintain control over the system for malicious purposes.

Rootkits are notoriously difficult to detect and remove due to their ability to conceal themselves within the operating system.

**ROOTKITS CLASSIFICATION CHARACTERISTICS**

1. **Persistent**: Activates each time the system boots.
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**

The payload refers to the malicious actions or effects of a virus or malware. It is the part of the malware that performs the intended harmful activities on the infected system, such as stealing data, deleting files, or causing system disruptions.

Payload are classified based on the damage or threat they bring to the system.

The payload of a virus defines what happens after it reaches the target.

The different classes of payload are:

❐ \_System Corruption - Causes damage to physical equipment such as Stuxnet worm. Targets specifc industrial control system software There are concerns about using sophisticated targeted malware for industrial sabotage.

❐ \_Attack Agents Bots - Attack Agents, known as bots, take over computers to launch attacks. They form botnets for coordinated action, such as DDoS attacks.

❐ \_Remote Control Facility -

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

❐ \_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 is a form of cyber-attack that utilizes social engineering to deceive users into divulging sensitive information by impersonating a trusted entity.

❐ \_Stealthing Backdoor - A stealthing backdoor, also known as a trapdoor, is a clandestine entry point within a program that grants unauthorized access, enabling attackers to circumvent security protocols.

Difficult to implement operating system controls.

❐ \_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.

**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

A screenshot of a computer software

Description automatically generated !!!!!! Important