**Malware Threats**

**Index:**

**Introduction to Malware:**

Malware is malicious software designed to harm, exploit, or disrupt systems. Common types include viruses (self-replicating code), worms (self-propagating malware), Trojans (disguised as legitimate software), ransomware (data-locking for ransom), and spyware (surveillance without consent). Notable examples includes Trojans, Backdoors, Rootkits etc.

**Different Ways for Malware to Enter a System:**

1. **Phishing Emails**: Malicious attachments or links in deceptive emails trick users into downloading malware.
2. **Infected Software Downloads**: Downloading software or files from untrusted sources can introduce malware.
3. **Vulnerabilities**: Exploiting security flaws in software or operating systems allows malware to enter.
4. **Removable Media**: Malware can spread via infected USB drives or external storage devices.
5. **Malicious Websites**: Visiting compromised or harmful websites can trigger malware downloads through drive-by downloads or exploits.

**Techniques to distribute malware on the web:**

Attackers distribute malware using various techniques, including exploiting web searches, deceiving users with clicks, and compromising trusted sites.

Three main ways to distribute malware:

1. **Black Hat SEO**: Manipulates search results to rank malicious pages highly, increasing the likelihood of user visits.
2. **Social Engineered Click-jacking**: Tricks users into clicking concealed malicious links or buttons that execute harmful actions.
3. **Compromised Legitimate Websites**: Embeds malware on genuine sites, spreading it to visitors unknowingly.

**Components of Malware:**

1. Crypter
2. Downloader
3. Dropper
4. Exploit
5. Injector
6. Obfuscator
7. Packer
8. Payload
9. Malicious Code

**Potentially Unwanted Application or Applications (PUAs):**

These are harmful applications that pose severe risks to the security and privacy of data.

Types of PUAS:

1. Adware
2. Torrent
3. Dialers

**Adware:**

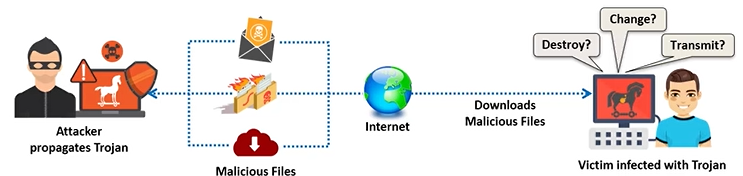
Adware is a type of software designed to display unwanted advertisements on users' devices. Typically, it generates revenue for the creator by automatically rendering ads. While not always harmful, it often hides within free applications, monitors browsing habits, and can annoy users with pervasive, intrusive pop-ups or banners.

**What are Advanced Persistent Threats?**

When the access to target network is for long time by the attacker. Advanced Persistent Threats (APTs) are prolonged, targeted cyberattacks where attackers maintain unauthorized access to a network for extended periods. Their goal is often espionage, data theft, or system manipulation, using sophisticated methods to avoid detection and maintain control over the network, exploiting vulnerabilities over time.

**What is a Trojan?**

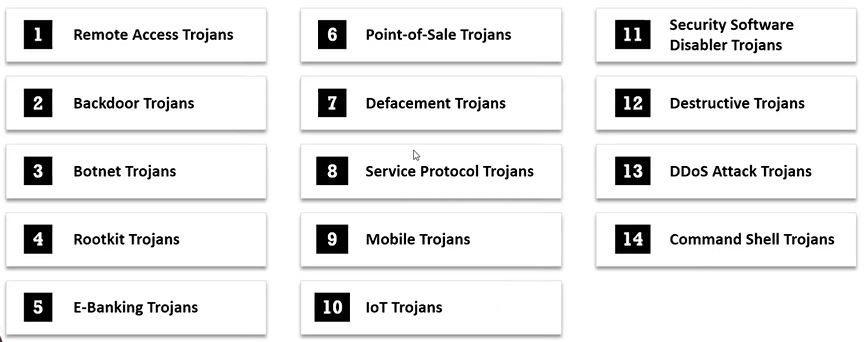
A Trojan (or Trojan horse) is a type of malicious software that disguises itself as a legitimate program or file. Once executed, it can compromise the security of a computer or network, stealing data, granting unauthorized access, or causing other damage, often without the user’s knowledge.



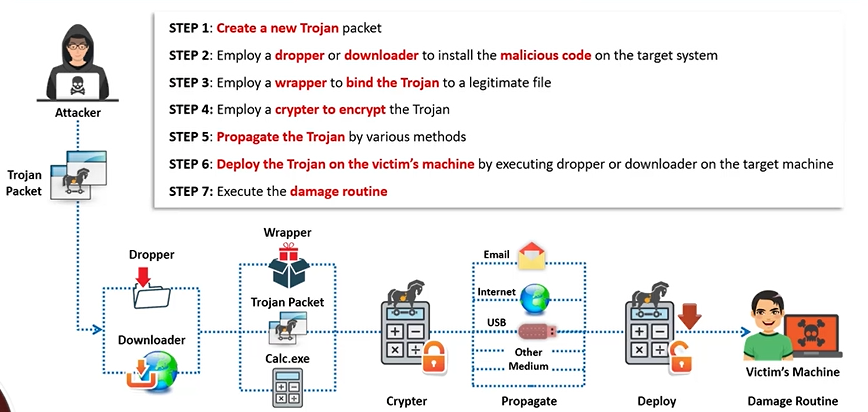
**How hackers use Trojans?**

Do whatever they want 😉

**Types of Trojans:**

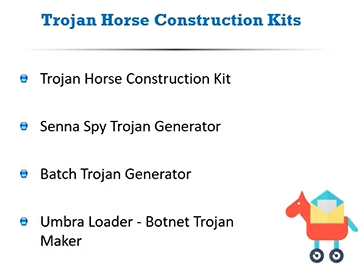
****

**How to infect systems using a Trojan?**

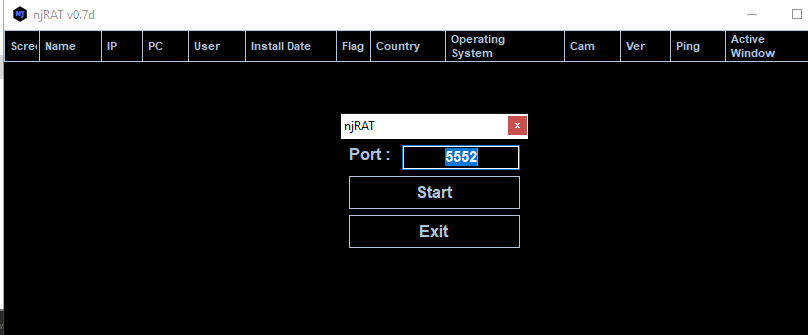
****

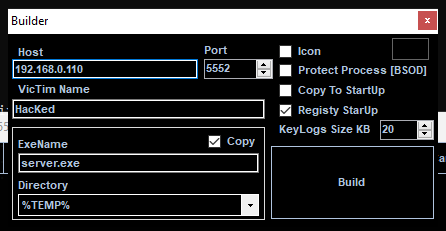
**Creating a Trojan:**

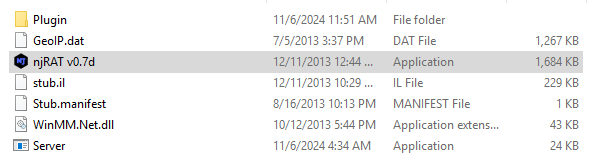
Trojan Horse construction kits help attackers to construct Trojan Horses of their choices.

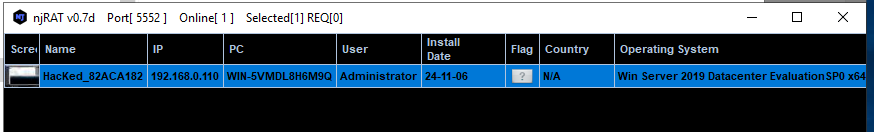


**Using njRAT:**

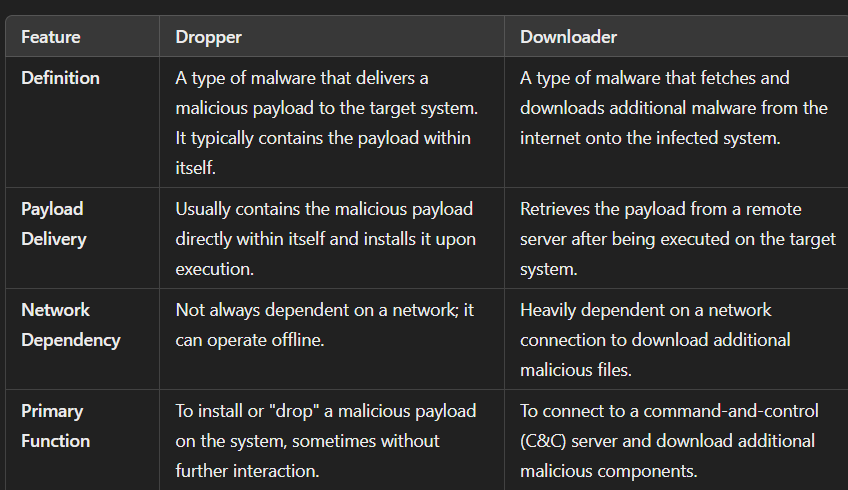
****

****

****

****

**Dropper vs Downloader:**

****

**Employing a Crypter:**

These are the software used by attackers to hide viruses, keyloggers or tools in any kind of file, to avoid antiviruses.

Some major are:

1. Bit crypter
2. Snip3
3. SwayzCryptor

**Propagating and deploying a Trojan:**

Major ways are:

1. Through emails
2. Through covert channels
3. Through proxy servers
4. Through USB/Flash drivers

**Exploit Kits:**

Exploit kits are automated tools used by cybercriminals to identify and exploit vulnerabilities in software on a target system, often through malicious websites. They deliver malware by exploiting weaknesses without needing user action beyond visiting a page.

**Introduction to viruses:**

A virus is malicious software that attaches itself to legitimate programs or files, replicating and spreading to other systems. It damages data, disrupts functions, and requires user action to activate.

**Characteristics of viruses:**

* **I**nfect other programs
* Transform themselves
* Encrypt themselves
* Alter data
* Self-replicate

**Purpose of creating viruses:**

* Research projects
* Damage networks or computers
* Gain remote access to a victim’s computer
* Financial benfits

**How to infect systems using a virus:**

**Creating a virus:**

A virus can be created in two different ways:

1. Writing a virus program
2. Using virus maker tools
3. Deadly virus maker
4. DELmE’s Batch Virus maker
5. JPS virus maker
6. TeraBIT virus maker

**Propagating and deploying a virus:**

Virus hoaxes are used to do so.

**Ransomware:**

Type of malware that restricts access to a computer system’s files and folders and demands online ransom payment.

Some famous are: Blackcat, cerber, NETWALKER, QNAPcrypt, Maze

**Computer worms:**

A **computer worm** is a self-replicating malware that spreads across networks without user action, exploiting security vulnerabilities to infect multiple devices autonomously, often causing network congestion or data loss.

A **computer virus** attaches itself to files or programs and spreads through user interaction, like file sharing. Unlike worms, viruses need a host to execute and typically spread more slowly.

**What is Fileless Malware?**

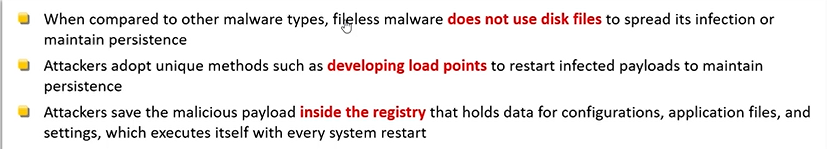
Fileless malware is a type of malicious software that operates entirely in a computer’s memory, leaving no trace on the hard drive. It exploits existing system tools or vulnerabilities to execute attacks, making it difficult to detect with traditional antivirus software. Often, it resides in RAM, disappearing upon reboot, evading standard defences.

It is used because:

1. **Stealth and Evasion**: Fileless malware avoids detection by traditional antivirus software, as it doesn’t leave a file on the disk.
2. **Persistence**: It leverages legitimate system tools, making it harder to identify and stop without disrupting regular processes.
3. **Speed of Infection**: Fileless attacks can rapidly exploit vulnerabilities in memory, achieving their goals quickly before systems detect or block them.

It can be launched via:

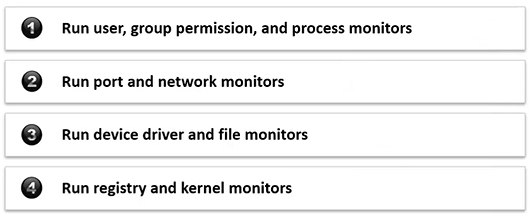
1. Document exploits
2. In-memory exploits
3. Script-based injection



**What is Sheep Dip Computer?**

Sheep dipping refers to the analysis of suspect files, incoming messages, etc. for malware.

What it do?

****

**Antivirus Sensor systems:**An antivirus sensor system is a security solution that detects, prevents, and removes malware by monitoring computer systems and networks for suspicious activity, leveraging advanced algorithms, real-time scanning, and threat intelligence to protect sensitive data and maintain system integrity.

**Introduction to malware analysis:**

It’s a kind of reverse engineering where the malware is analysed to determine its origin, functionality and potential impact.

Why malware analysis?

1. To determine exactly what happened.
2. To identify indicators of compromise
3. To identify the exploited vulnerability

Types of malware analysis:

1. Static malware analysis - code analysis
2. Dynamic malware analysis - behavioural analysis

**Static Malware Analysis:**

In this we don’t run the malware code, so there is no need to create a safe environment.

**SMA: File fingerprinting**

It is the process of computing the hash value for a given binary code.

Some major tools are:

1. Mimikatz
2. HashCalc
3. Hashdeep
4. MD5sums
5. HashMyFiles

**SMA: Local and Online malware scanning**

It involves scanning the binary code locally using well-known and up-to-date antivirus software.

Some tools to do so are:

1. Virustotal
2. Hybrid analysis
3. Cuckoo sandbox
4. Jotti



**SMA: Performing Strings search**

Strings communicate information from the program to its user. Analyse embedded strings of readable text within the program’s executable file.

String searching tools:

1. FLOOS
2. BInText
3. FIleSeek
4. Hex Workshop

**SMA: Identifying Packing/Obfuscation Methods**

Compressing the malware using packers allow attackers to modify the malware to avoid detection. It basically complicates the task for reverse engineers.

Tools to do so:

1. PEid
2. Macor\_pack
3. UPX

**SMA: Finding the portable executable information**

PE format is the executable format used on the Windows OS. Analysing the metadata of PE files helps to give many information.

Major tools are:

1. PE explorer
2. PEView
3. Pescan
4. Resource Hacker

**SMA: Identifying File dependencies**

Check the dynamically linked list in the malware executable file. Finding out all the library functions may allow you to estimate what the malware program can do.

Some tools to do so are:

1. Dependency Walker
2. Synk
3. Dependency-check

**SMA: Malware Disassembly**

It involves the disassemble of binary code and analyze the assembly code instructions.

Disassembling and Debugging Tools:

1. Ghidra
2. IDA pro
3. Radare
4. OllyDbg

**Dynamic malware analysis:**

In this the malware is executed on a system to understand its behaviour after infection.

It consists of two stages:

1. System baselining – includes taking snapshot of the picture at the time of malware analysis to begun.
2. Host Integrity Monitoring – includes taking snapshot of tools before and after implementing the malware.

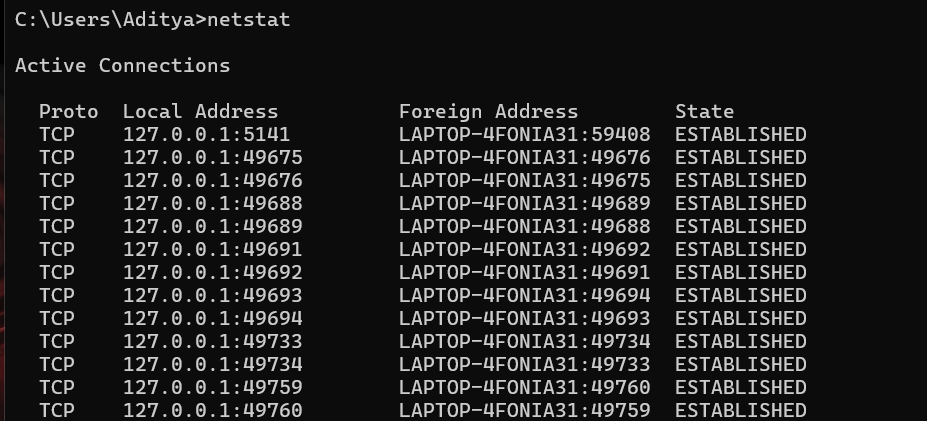
**Dynamic Malware analysis: Port Monitoring**

Malware programs corrupt the system and open system input/output ports to establish connections with remote systems, networks, or servers to accomplish various malicious tasks

Use port monitoring tools such as netstat, and TCPView to scan for suspicious ports and look for any connection established to unknown or suspicious IP addresses

Port monitoring tools:

1. Port Monitor
2. Netstat
3. TCP view
4. Cuu Ports



**Dynamic Malware analysis: Process Monitoring**

We can use process monitoring tools like process monitor to scan for suspicious processes who had hided themselves as genuine Windows services.

Some tools to do so:

1. Process monitor
2. Process explorer
3. OpManager
4. Monit

**Dynamic Malware analysis: Registry Monitoring**

Registry monitoring tools like regshot can be used to examine the changes made by the malware to the system’s registry.

Popular tools are:

1. Regshot
2. Jv16 PowerTools
3. RegScanner

**Dynamic Malware analysis: Windows Services Monitoring**

We can use Windows services monitoring tools such as Windows Service Manager (SrvMan) to trace malicious services initiated by the malware.

Tools:

1. SrvMan
2. Service+
3. Process Hacker

**Dynamic Malware analysis: Startup Programs Monitoring**

We can use tools like Autoruns for windows to detect suspicious startup programs and processes.

Tools:

1. Autoruns for windows
2. WinPatrol

**Dynamic Malware analysis: Event Logs Monitoring/Analysis**

Log analysis is a process of analysing computer-generated records or activities to identify malicious or suspicious events.

Tools:

1. Splunk
2. Loggly
3. Solarwinds

**Dynamic Malware analysis: Installation Monitoring**

It will help to detect hidden and background installations that the malware performs.

Tools:

1. SysAnalyzer
2. Mirekusoft install monitor
3. Comodo programs manager

**Dynamic Malware analysis: Files and Folders Monitoring**

Tools like PA File Sight can be used to detect changes in system files and folders.

Tools:

1. PA File Sight
2. Verisys
3. Tripwire File Integrity an Change Manager

**Dynamic Malware analysis: Device Divers Monitoring**

Tools:

1. DriverView
2. Driver Booster
3. Driver Receiver

**Dynamic Malware analysis: Network Traffic Monitoring**

Tools:

1. SolarWinds NetFlow Traffic Analyzer
2. Caspa Network Analyzer
3. Wireshark

**Dynamic Malware analysis: DNS Monitoring**

Tools:

1. DNS Query sniffer
2. DNS stuff
3. Ultra DNS

**Dynamic Malware analysis: API Calls Monitoring**

Tools:

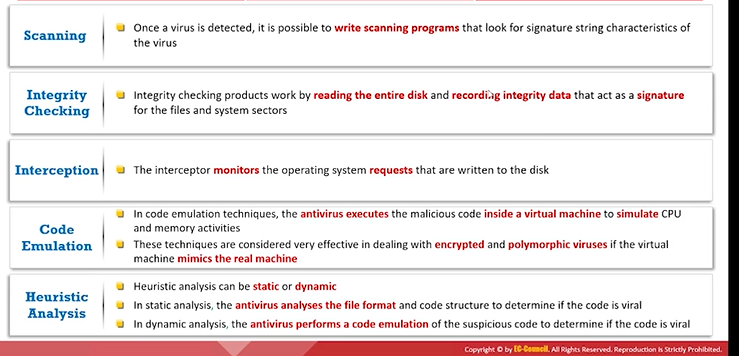
1. API Monitor
2. APImetrics
3. Runscope

**Dynamic Malware analysis: System calls Monitoring**

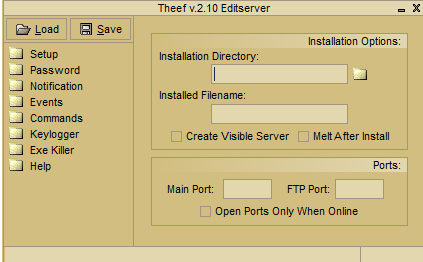
Tools:

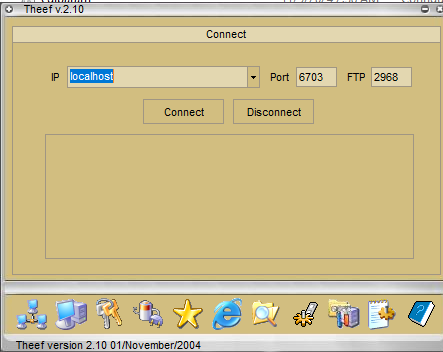
1. Strace

**Virus detection methods:**

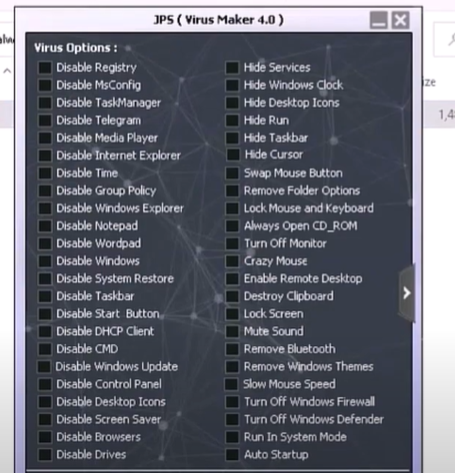
****

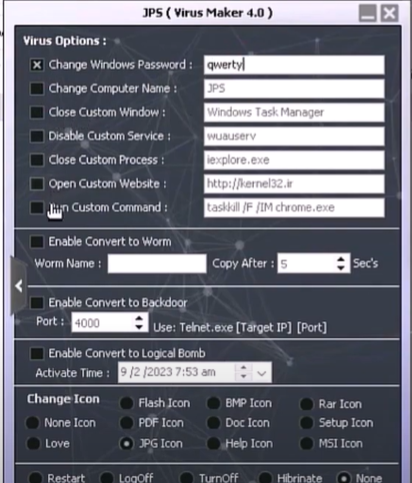
**Using the THEEF RAT:**

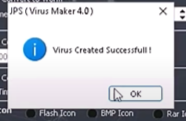
****

****

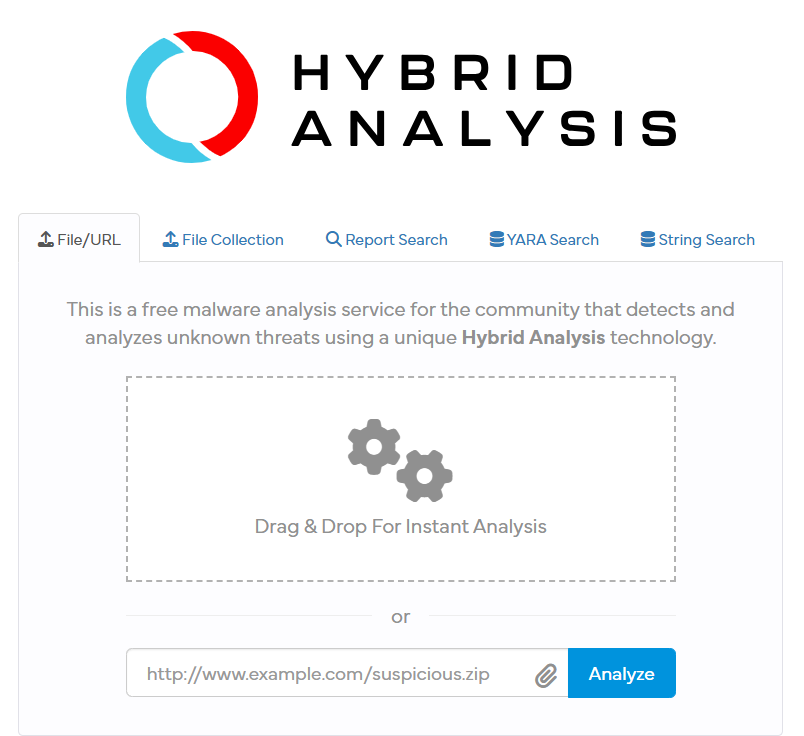
**Using the JPS virus maker tool:**

****

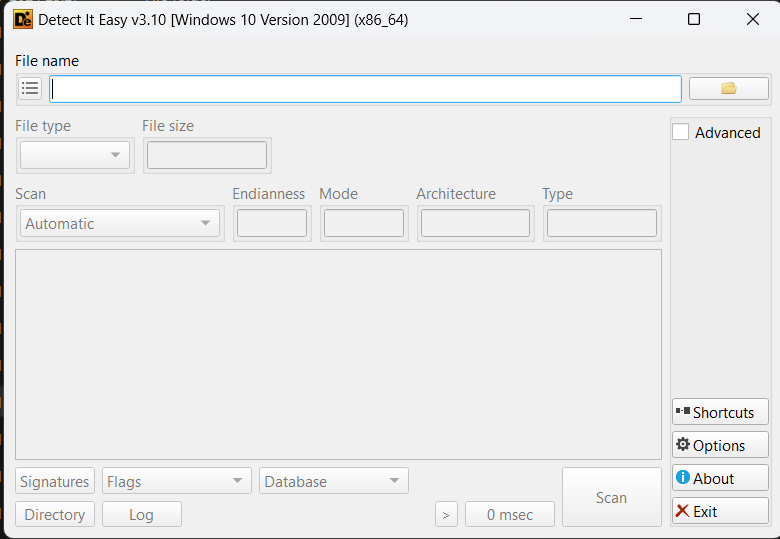
****

****

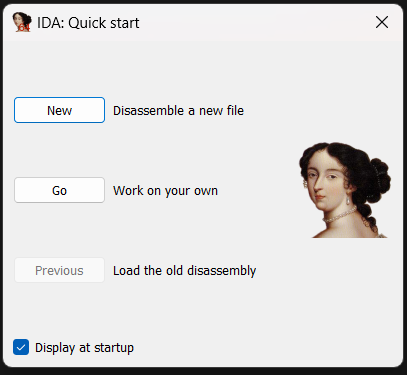
**Perform malware scanning using Hybrid analysis:**

****

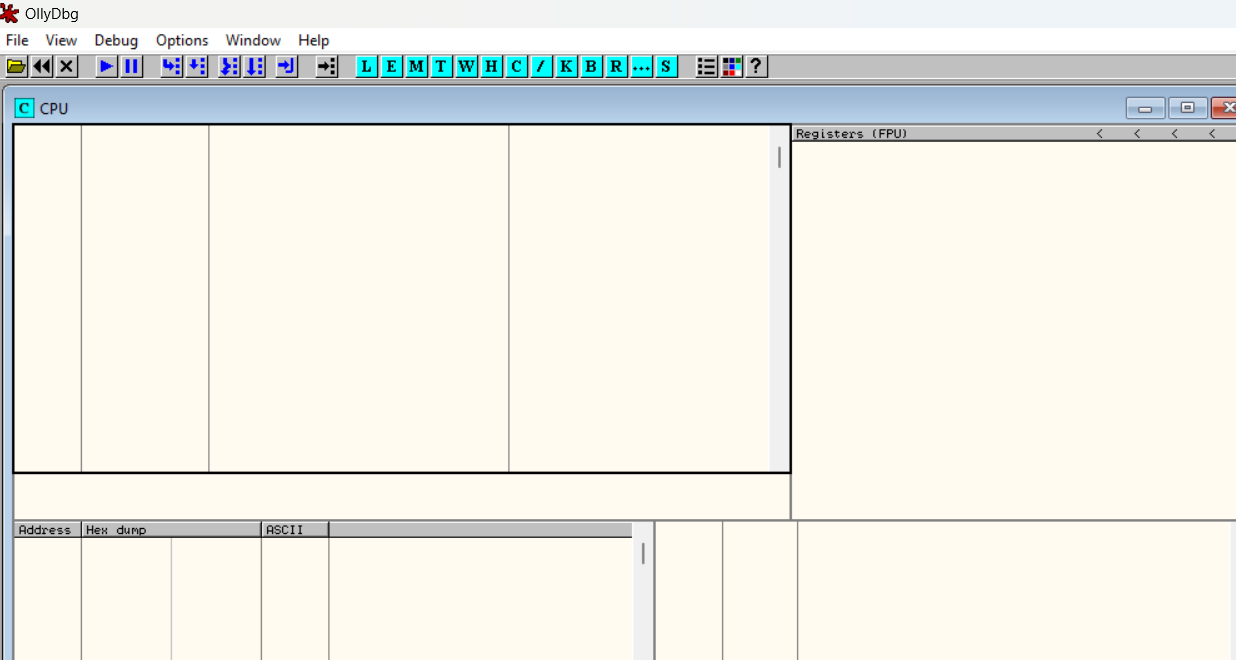
**Analyse ELF executable file using detect it easy (DIE):**

****

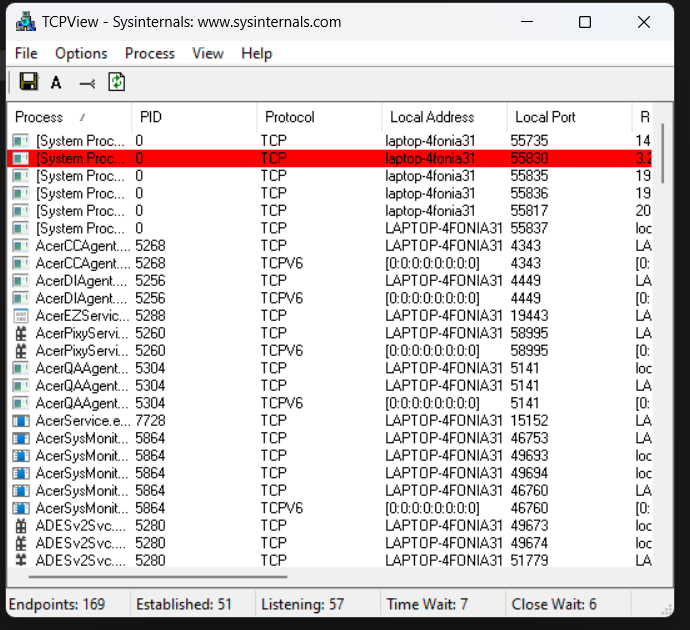
**Using IDA:**

****

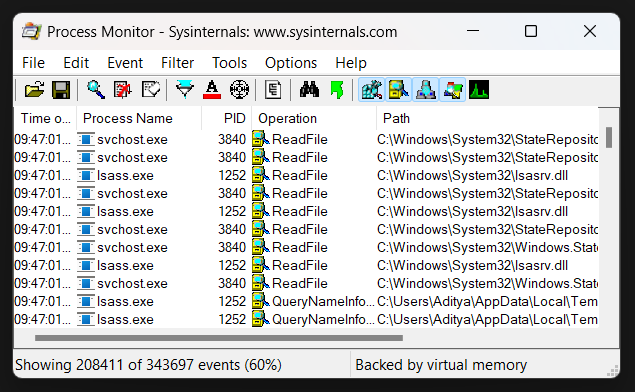
**Using OllyDBG:**

****

**Using TCPView:**

****

**Process monitor:**

****