Name : kunal Jawale

Module 7 : Malware Threats

Malware, or malicious software, poses a significant threat to cybersecurity, encompassing various types of attacks designed to damage or steal data. These attacks can be delivered through various channels, including email attachments, infected websites, and compromised software downloads. Malware can be used to steal sensitive information, encrypt files for ransom, control a network of infected devices, or disrupt system operations.

Types of Malware:

- **Viruses:** Malware that requires a host file to spread and replicate.
- **Worms:** Self-replicating malware that can spread rapidly across networks without requiring a host file.
- **Trojans:** Disguised as legitimate software, Trojans deliver a malicious payload when executed.
- **Ransomware:** Encrypts a victim's files and demands payment for the decryption key.
- **Spyware:** Collects information about a user's activity without their knowledge or consent.
- **Adware:** Displays unwanted advertisements and can lead to further malware infections.
- **Rootkits:** Hide malware activity and gain administrator-level access to a system.
- **Botnets:** Networks of compromised computers controlled by a single attacker.

Common Malware Attack Vectors:

- **Phishing:** Deceptive emails or websites designed to trick users into revealing personal information or installing malware.
- **Social Engineering:** Manipulating individuals to perform actions that compromise security.
- **Exploiting Vulnerabilities:** Taking advantage of weaknesses in software or operating systems to install malware.
- **Infected Websites:** Visiting websites that have been compromised or have malicious advertising.
- **Downloading from Untrusted Sources:** Installing software from non-official or questionable sources.

Name : kunal Jawale

Impact of Malware Attacks:

- **Data Breaches:**

Theft of sensitive information like passwords, financial details, and personal data.

- **System Disruption:**

Malware can cause a system to become unstable, unresponsive, or completely unusable.

- **Financial Losses:**

Ransomware attacks, data breaches, and system downtime can result in significant financial costs.

- **Reputational Damage:**

Malware incidents can damage a company's reputation and erode customer trust.

Prevention and Mitigation:

- **Install and Update Antivirus Software:** Regularly update your antivirus software to protect against the latest threats.
- **Be Cautious of Emails and Websites:** Be wary of suspicious emails, links, and websites, and avoid clicking on them.
- **Use Strong Passwords:** Choose strong and unique passwords for all online accounts.
- **Keep Software Updated:** Regularly update your operating system and software to patch vulnerabilities.
- **Implement Security Controls:** Use firewalls, intrusion detection systems, and other security measures.
- **Educate Users:** Train employees about common malware threats and how to stay safe online.

Name : kunal Jawale

Trojans

A Trojan is a type of malware that tricks users into installing malicious software that can damage or steal data. Trojans are also known as Trojan horses.

	Trojan
What it is	A malicious program that pretends to be legitimate software
How it works	Disguises itself as a useful program, like a game, utility, or antivirus program
What it does	Steals data, damages files, or takes control of your computer
How it spreads	Through email attachments, text messages, bogus websites, or free programs
How to protect against it	Run a full virus scan on your computer

Trojans can be used for a variety of malicious purposes, including:

- **Stealing data**: Trojans can steal sensitive data, passwords, and other information
- **Monitoring activity**: Trojans can monitor your keyboard strokes and other activity
- **Creating backdoors**: Trojans can create access points that allow cybercriminals to remotely control your computer
- **Disrupting systems**: Trojans can delete or modify data, block data, or disrupt system performance
- **Conducting DDoS attacks**: Trojans can be used to create traffic that crashes other systems

- **Pretending to be antivirus software**: Trojans can pretend to detect viruses and other malware, and then trick you into paying for security software
- **Encrypting files**: Trojans can encrypt some or all of your files, making your device unusable or inaccessible

The term "Trojan" comes from the ancient Greek story of the Trojan Horse that led to the fall of Troy.

/ here are some types of trojan

O Netbus1.7 :-

NetBus 1.7 is an older Trojan horse malware, not a current cybersecurity concern. It was a popular example of early remote access Trojans (RATs). While it's historical, understanding NetBus's functionality can be helpful in identifying similar threats today.

How NetBus 1.7 Worked:

- **Remote Access:**

  NetBus allowed an attacker to remotely control an infected computer, like a backdoor.

- **Functionality:**

  It could perform various actions on the victim's machine, including:

- Displaying the computer's screen to the attacker.
- Executing commands on the computer.
- Stealing data, such as passwords or files.
- Even locking or disabling the infected computer.
- **Spread:**
  The original NetBus was spread through various methods, including email attachments and peer-to-peer networks.

Why it's a Historical Example:

- **Outdated Technology:**

  NetBus relies on older protocols and techniques that are no longer widely used by cybercriminals.

- **Easily Detectable:**

Modern security software can readily identify and remove NetBus, which is why it's no longer a significant threat.

- **More Advanced Trojans Exist:**
  Cybercriminals have moved on to more sophisticated malware like RATs with enhanced capabilities and better evasion techniques.

Why Understanding NetBus is Still Relevant:

- **Learning About RATs:**

  NetBus provides a basis for understanding how RATs work and what capabilities they offer.

- **Identifying Modern Threats:**

  Recognizing the signs of a backdoor or remote access malware can help in detecting and preventing attacks from more recent Trojans.

- **Cybersecurity Education:**
  Studying NetBus can be a valuable tool in educating individuals about the dangers of malware and how to protect themselves.

In essence, NetBus 1.7 is a historical example of a Trojan horse, specifically a remote access Trojan (RAT). While no longer a major threat, understanding its operation can be helpful in understanding the broader category of Trojans and the evolution of cybersecurity threats.

O njRAT :-

NJRat has the ability to spread itself in a few different ways. While its primary infection vectors are phishing attacks and drive-by downloads, it also has the ability to spread itself via infected USB drives. The choice of propagation method can be set using the malware's command and control (C2) software.

Once installed on a target system, the malware is designed to allow the attacker to remotely access and control that system.

NJRat boasts various capabilities, including:

- Keylogging
- Webcam Access

Name : kunal Jawale

- Theft of credentials stored in browsers
- File uploads and downloads
- Process and file manipulations
- Shell command execution
- Registry modification
- Screen captures
- Viewing the desktop of the infected computer
- Theft of cryptocurrency and payment data from crypto wallet apps
- NJRat also uses various techniques to evade detection on an infected system. For example, the malware will disguise itself as a critical process, making users less likely to kill it for fear of rendering their system unusable. It also actively defends itself by deactivating endpoint security software and detecting if it is running in a virtualized environment, making it more difficult for security researchers to analyze.
- NJRat is also a modular malware variant with the ability to download additional code from Pastebin and similar sites. This enables the malware to expand its capabilities or to act as a dropper for other types of malware once it has established a foothold on an infected device.

Name : kunal Jawale

Virus

A computer virus is a type of malware that can damage or destroy data, files, and software. Viruses can spread from one computer to another, and they can be very harmful.

What is a Virus in Cybersecurity?

A **computer virus** is a type of **malicious software (malware)** designed to **infect, replicate, and spread** from one computer to another. A virus attaches itself to legitimate programs or files and executes when the infected program is run or the file is opened. Its primary aim is to disrupt operations, corrupt or steal data, and sometimes render systems inoperable.

Name : kunal Jawale

How Does a Virus Work?

1. **Infection:**
   - The virus attaches itself to a host file (e.g., .exe, .doc, .xls).
   - It can be spread through:
     - Email attachments
     - Downloaded software
     - Infected USB drives
     - Malicious websites
2. **Replication:**
   - When the infected host is executed, the virus activates and begins replicating itself.
   - It may attach to other files or programs, spreading further.
3. **Activation:**
   - Some viruses activate immediately, while others lie dormant and trigger based on specific conditions (e.g., a certain date or action).
4. **Payload Execution:**
   - The virus performs its malicious action, which may include:
     - Deleting or corrupting files
     - Stealing sensitive information (passwords, banking details)
     - Slowing down system performance
     - Hijacking system resources

Types of Computer Viruses:

1. **Boot Sector Virus:**
   - Infects the master boot record (MBR) of a hard disk.
   - Activates during system startup, before the OS loads.
2. **File Infector Virus:**
   - Attaches itself to executable files (.exe, .com).
   - Spreads when the infected program is executed.
3. **Macro Virus:**
   - Written in macro languages (like VBA for Microsoft Office).
   - Spreads through infected Word documents or Excel spreadsheets.
4. **Polymorphic Virus:**
   - Changes its code slightly each time it replicates.
   - Makes it harder for antivirus software to detect.
5. **Resident Virus:**
   - Embeds itself into a computer's memory.
   - Can execute malicious actions even if the original infected file is deleted.
6. **Multipartite Virus:**

- Can spread in multiple ways—infects both the boot sector and executable files.

Symptoms of Virus Infection:

- Unexpected pop-up messages
- Slow system performance
- Frequent crashes or system freezes
- Missing or corrupted files
- Unknown programs launching on startup
- Increased network activity without reason

Prevention Measures:

1. **Use a Reliable Antivirus Software:**
   - Keep it updated to recognize new virus signatures.
2. **Avoid Opening Unknown Attachments:**
   - Be cautious with email attachments, even from trusted sources.
3. **Enable Firewall Protection:**
   - Prevent unauthorized access to your system.
4. **Keep Software Updated:**
   - Apply security patches regularly to fix vulnerabilities.
5. **Disable AutoRun on External Devices:**
   - Prevent viruses from spreading through USBs or CDs automatically.
6. **Backup Data Regularly:**
   - Protect your data in case of an attack.
7. **Do Not Download from Untrusted Sources:**
   - Avoid pirated software and suspicious websites.

Computer virus

How it spreads Attaches to a program or file, and replicates itself

---

How it's activated When the program or file is opened

Name : kunal Jawale

How it harms Corrupts or destroys data, steals passwords, logs keystrokes, and more

---

How to prevent Use antivirus software, don't click on suspicious links, and update your software regularly

---

Some types of viruses include:

- ILOVEYOU
- CryptoLocker
- MyDoom
- Storm Worm
- Sasser & Netsky
- Anna Kournikova virus
- Slammer
- Stuxnet

You can protect your computer from viruses by:

- Installing antivirus software
- Keeping your software up to date
- Scanning removable media before opening files
- Enabling email security features
- Enabling firewall protection
- Running a full virus scan regularly
- Ensuring automatic updates are turned on

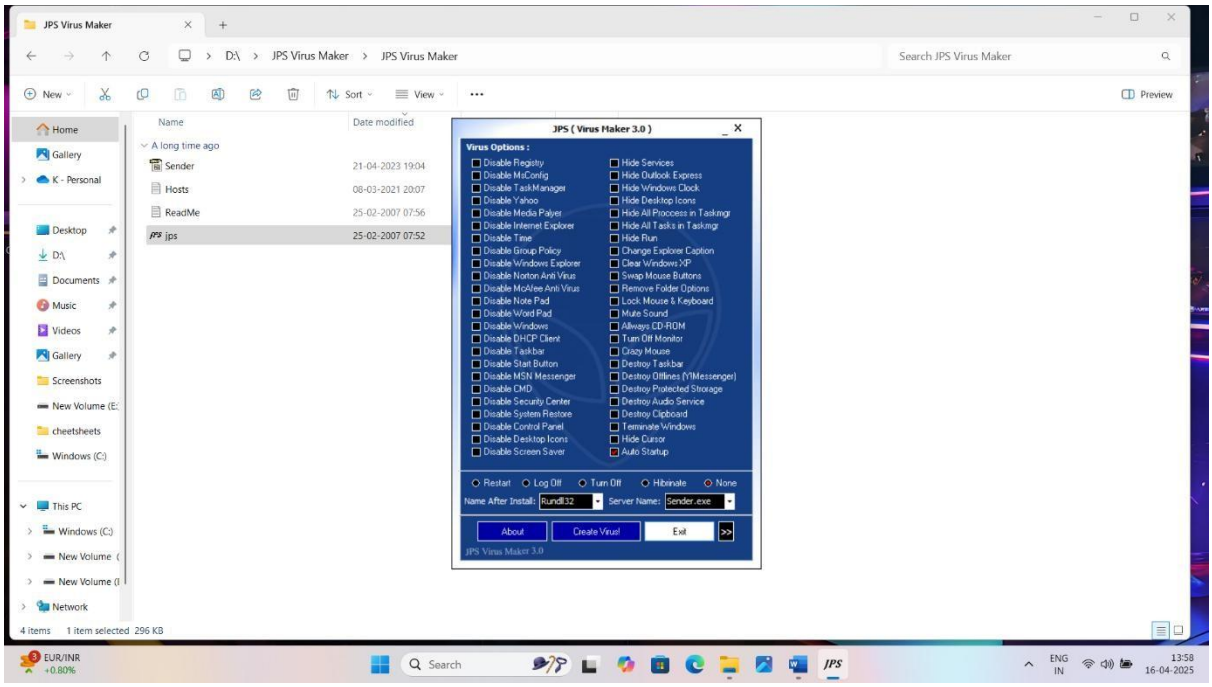
➢ JPS virus maker :-

Using JPS virus maker you create multiple types of viruses and its very dangerous .

In the following image that show you using

Name : kunal Jawale

JPS virus maker what type of options is their



Malware Analysis

Malware analysis is the process of examining malicious software (like viruses, worms, or ransomware) to understand its functionality, behavior, and potential impact. This helps security professionals identify threats, detect indicators of compromise (IoCs), and develop countermeasures to prevent future attacks.

Key aspects of malware analysis include:

- **Static Analysis:**

  Examining the malware's code without executing it, often through techniques like disassembly and decompilation to understand its logic, functions, and algorithms.

- **Dynamic Analysis:**

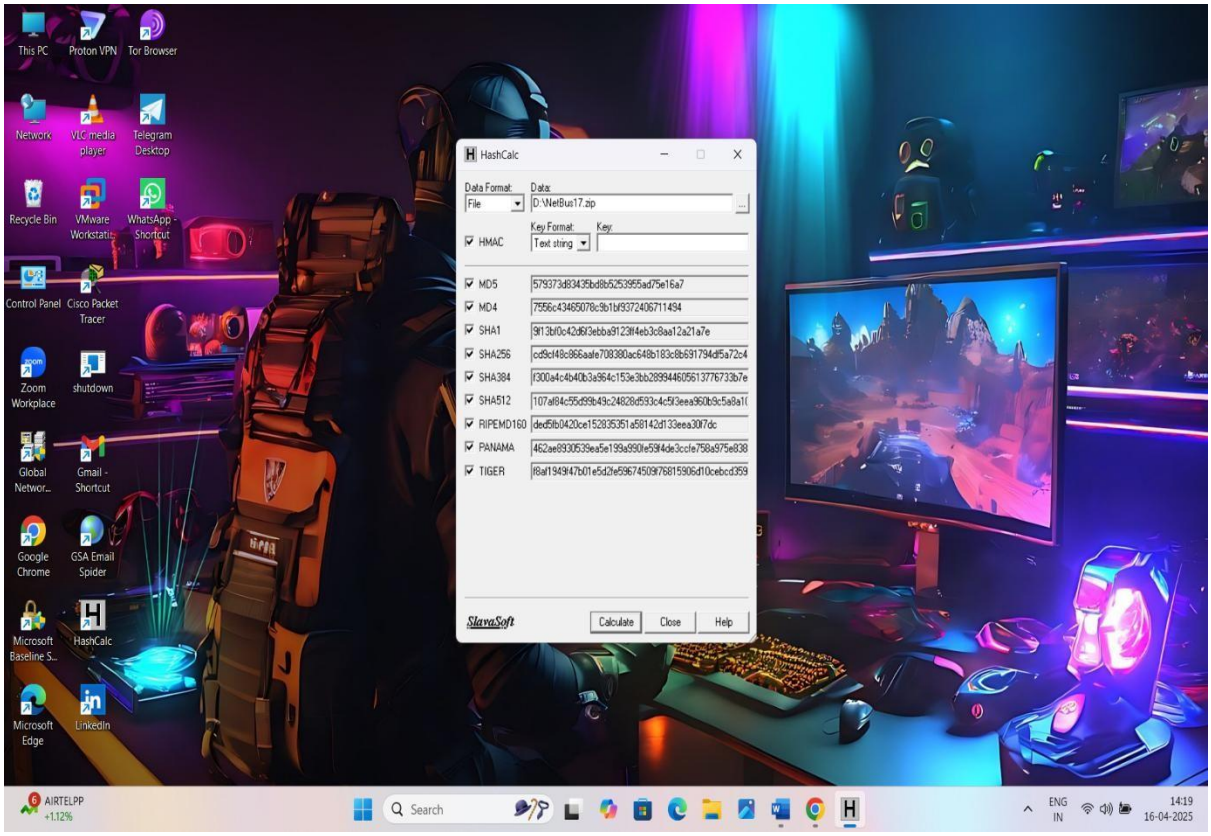
  Observing the malware's behavior in a controlled environment, such as a virtual machine, to understand how it interacts with the system, what resources it uses, and its communication patterns.

In essence, malware analysis is crucial for cybersecurity professionals to effectively detect, analyze, and mitigate the risks posed by malicious software. It provides the knowledge and insights needed to protect systems and networks from evolving cyber threats.

Name : kunal Jawale

Static analysis

- File printing :- using Hashcalc you got to know file is real or anyone is interrupted file or not .



- **Hybrid malware analysis :-**

What is Hybrid Malware Analysis?

Hybrid Malware Analysis is a **comprehensive method** for investigating malware by combining both **Static Analysis** and **Dynamic Analysis** techniques. This dual approach provides deeper insights into the behavior, structure, and potential impact of the malicious software.

Why Hybrid Malware Analysis?

Name : kunal Jawale

Individually, static and dynamic analysis have limitations:

- **Static Analysis** can identify code signatures and structure without execution, but it **cannot detect runtime behaviors** like network connections or system changes.
- **Dynamic Analysis** observes the malware in action, identifying its **real-time impact on the system**, but it can be **evasive** if the malware detects a virtual environment or sandbox.

Hybrid Analysis bridges these gaps by:

1. **Identifying code-level threats** and **runtime behavior**.
2. Detecting obfuscated code or encrypted payloads that are only visible during execution.
3. Mapping out the complete kill chain of the malware, including:
    - **Infection Vector → Execution → Propagation → Persistence → Data Exfiltration**.

Phases of Hybrid Malware Analysis:

🔍 1. Static Analysis (Pre-Execution):

- **File Examination:** Analyzing the file type, headers, imports, and exports.
- **Hash Calculation:** Generating MD5, SHA-1, or SHA-256 hashes for identification.
- **String Analysis:** Searching for readable strings like URLs, IP addresses, registry paths.
- **Dependency Analysis:** Inspecting libraries, APIs, and linked DLLs.
- **Disassembly:** Reviewing the assembly code to understand logic without execution.

⚙️ 2. Dynamic Analysis (Runtime Monitoring):

- **Behavior Observation:** Executing the malware in a **sandboxed environment** to monitor:
    - File creation/modification
    - Network communications (HTTP, FTP, DNS requests)
    - Registry changes
    - Process creation and memory injections
- **Network Analysis:** Capturing packets to identify C2 (Command and Control) servers.

- **System Calls:** Monitoring low-level system calls to detect privilege escalation or process manipulation.

🔄 3. Correlation and Reporting (Post-Analysis):

- **Compare and Correlate Results:** Analyze data from both static and dynamic phases.
- **Behavioral Indicators:** Create Indicators of Compromise (IOCs) for detection.
- **Generate Reports:** Document the findings, including attack vector, persistence mechanisms, and network indicators.

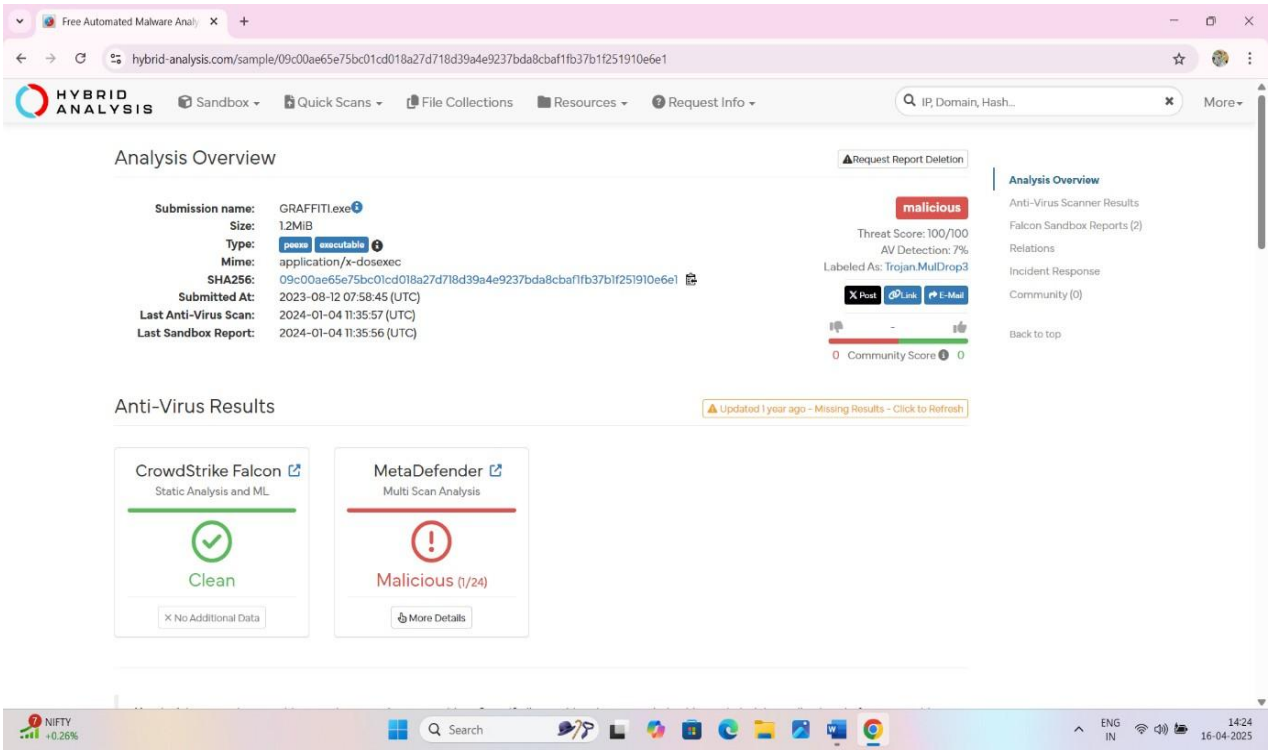
Tools Used for Hybrid Malware Analysis:

1. **Cuckoo Sandbox:** Automates dynamic malware analysis with detailed reports.
2. **VirusTotal:** Performs both static and dynamic analysis using multiple engines.
3. **Hybrid Analysis (by CrowdStrike):** Online platform for hybrid analysis of malware.
4. **PEiD, Ghidra, IDA Pro:** For static analysis of executables.
5. **Wireshark:** For network packet analysis during runtime.
6. **Procmon & Regshot:** To monitor process and registry changes.

Advantages of Hybrid Analysis:

1. **Better Detection Accuracy:** Cross-verifies static indicators with real-time behavior.
2. **Evasion Resistance:** Captures runtime behaviors that may bypass static checks.
3. **Enhanced Threat Intelligence:** Builds a more complete profile of the malware's impact.
4. **Faster Incident Response:** Identifies critical attack vectors and persistence mechanisms.

Name : kunal Jawale

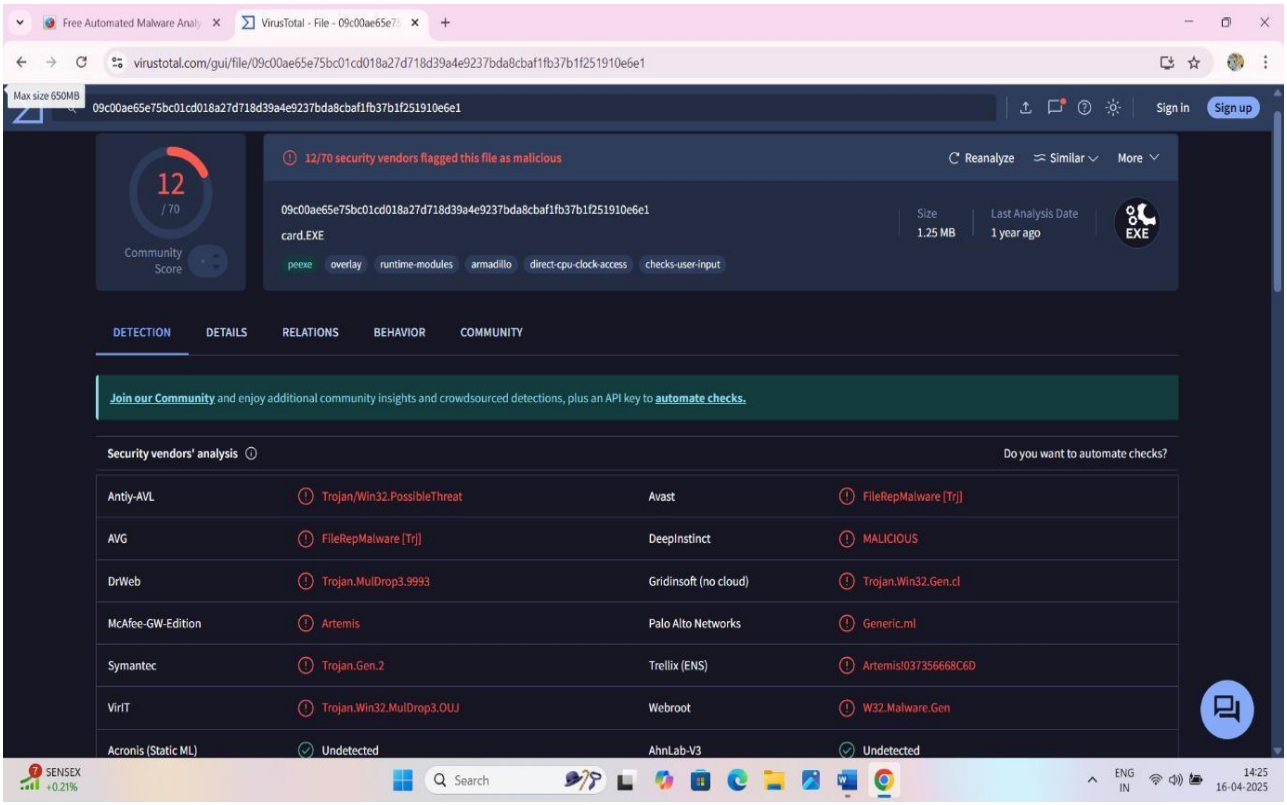


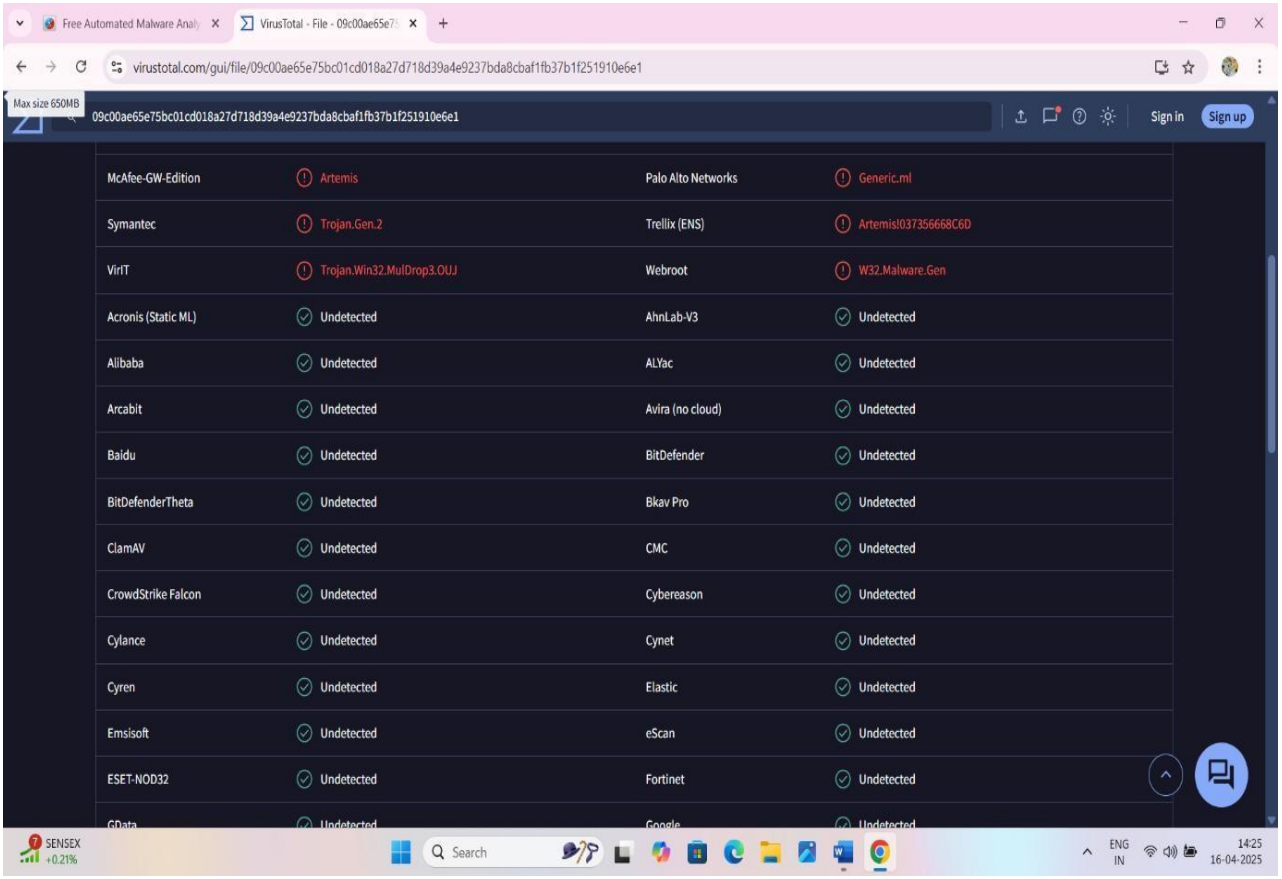
· Virustotal.com :-

VirusTotal provides several benefits for users seeking to analyze potentially malicious files and URLs. It leverages multiple antivirus engines and scanners to detect malware, and it also offers advanced analysis capabilities, including static and dynamic analysis, and metadata extraction. This allows users to gain a deeper understanding of the nature of a file or URL, aiding in threat detection and incident response.

Virus Total is an online service that analyzes suspicious files and URLs to detect types of malware and malicious content using antivirus engines and website scanners. It provides an API that allows users to access the information generated by VirusTotal.

Name : kunal Jawale





in the given image show you scan 70 types of antivirus and malicious file detected .

Name : kunal Jawale

O Die.exe :-

"die.exe" refers to a file associated with the Detect It Easy (DiE) tool, a program used for file type identification and analysis. It's primarily used by cybersecurity experts and reverse engineers to analyze files, including malware, by identifying their structure and format. DIE can also be used to identify signs of packing or other modifications to a binary file.

Here's a more detailed breakdown:

- **File Type Identification:**

  DIE can determine the type of a file by analyzing its contents, recognizing various formats like PE (Windows), ELF (Linux), MACH (MacOS), and others.

- **Signature and Heuristic Analysis:**

  It uses both signature-based and heuristic methods to identify file types, supporting a wide range of executable and archive formats.

- **Malware Analysis:**

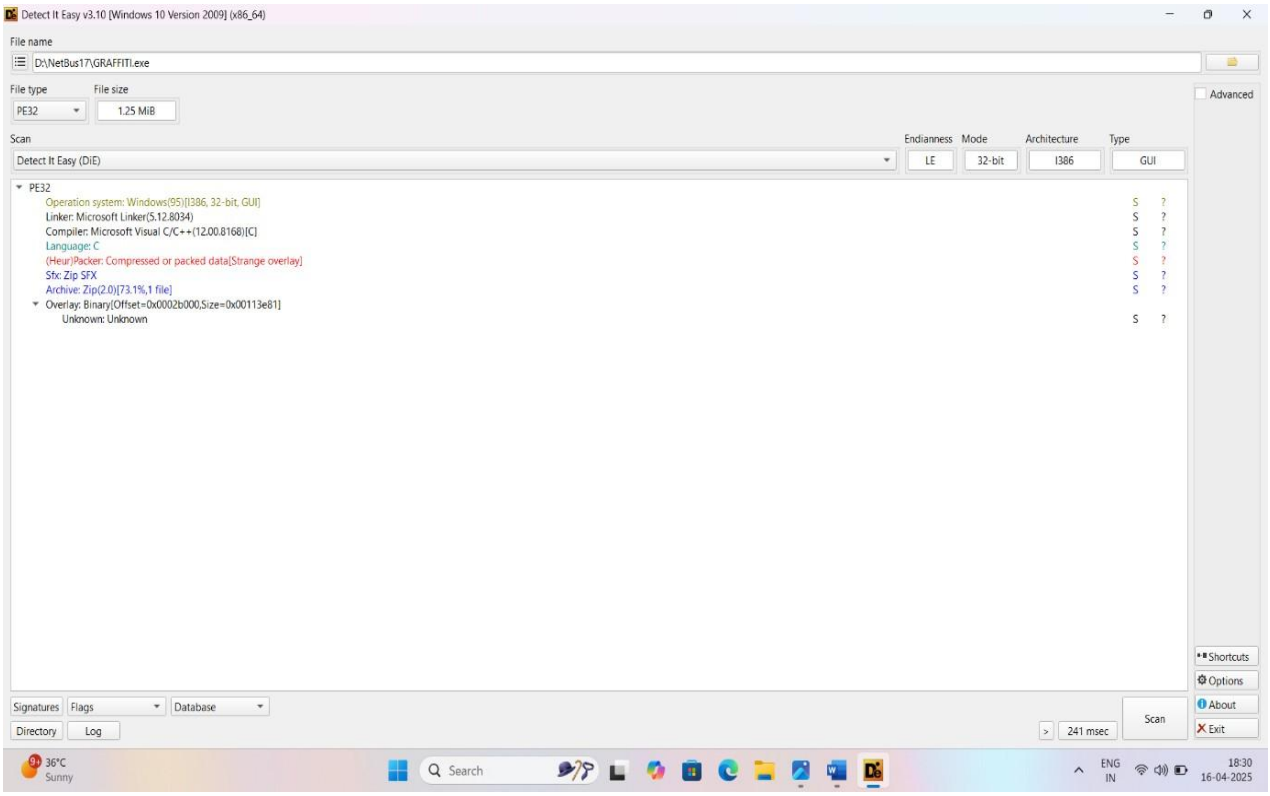
  DIE is frequently used in reverse engineering and malware analysis to understand the structure and behavior of suspicious files.

- **Open Architecture:**

  DIE's architecture is open, allowing users to add or modify detection algorithms using scripts, similar to JavaScript.

- **Multiple Versions:**
  DIE exists in various versions (basic, lite, console) that share the same signatures, stored in a "db" folder.

Name : kunal Jawale



IDA free :-

IDA Free is a free version of IDA Pro that allows users to disassemble and decompile x86 and x64 binaries for noncommercial use. It is a powerful tool for reverse engineering, malware analysis, and software vulnerability research.

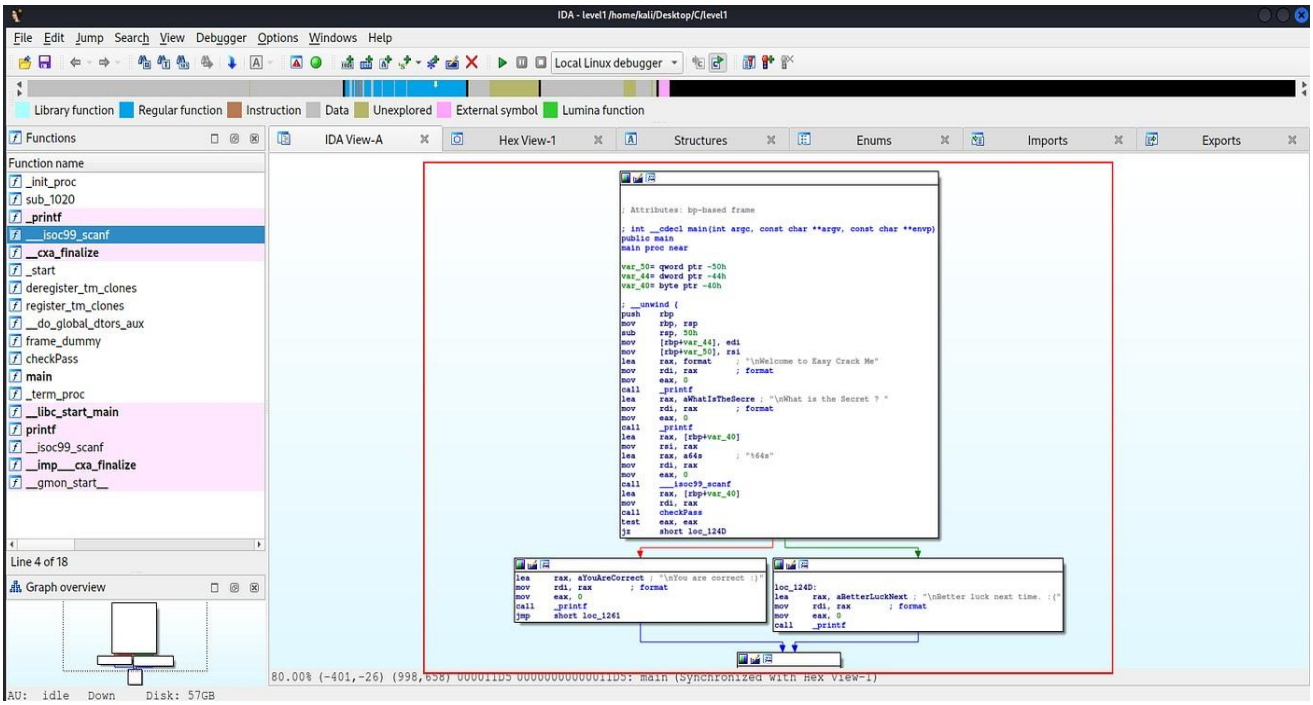
Here's a more detailed look at its uses:

1. Reverse Engineering: IDA Free is primarily used for reversing the engineering process, meaning to understand how a program works by analyzing its disassembled code.
2. Malware Analysis: Security professionals and researchers use IDA Free to analyze malicious software, identify vulnerabilities, and understand how malware functions.
3. Software Vulnerability Research: By examining the disassembled code of software, researchers can find security flaws and vulnerabilities that could be exploited.
4. Educational Purposes: IDA Free is also a valuable tool for teaching students the fundamentals of reverse engineering and security analysis.
5. Limitations:
    - **Non-Commercial Use:** IDA Free is only for non-commercial use, meaning it cannot be used to earn money or for business purposes.

- **Limited Architecture Support:** It primarily supports x86 and x64 architectures.
- **Feature Set:** It has a limited feature set compared to the full version of IDA Pro, including limited plugin support and scripting capabilities.

6. Cloud-Based Decompiler: IDA Free includes a cloud-based decompiler, allowing users to convert machine code into a more readable C-like pseudocode.
7. Debugging: While IDA Free is primarily a disassembler, it can also be used for debugging, offering features to assist in error detection and correction.

For commercial use or accessing a wider range of features, you should consider the IDA Pro subscription plans



Dynamic malware analysis

There are two types of dynamic malware analysis

Name : kunal Jawale

1 . **system baselining** :-

Baselining refers to the process of capturing a system state at the time the malware analysis begins. This can be used to compare the systems state after executing the malware file,which will help to understand the changes that the malware has made across the system.

2 . **Host integrity monitoring** :-

This is the process of studing the changes that have taken place across the system or a machine after series of action or incidents. It involves using the same tools to take snapshot of the system before and after the incident.

/ here are some tools for dynamic malware analysis

- **Regshot :-**

Regshot is a tool used to capture and compare snapshots of the Windows registry, particularly for analyzing changes made by malware or other software. It allows you to take a "first shot" of the registry, then make changes (like running malware or installing a program), and then take a "second shot". Comparing the two snapshots reveals the registry modifications.

Here's a more detailed breakdown of its uses:

- **Malware Analysis:**

  Regshot is valuable for identifying registry changes that malware makes during execution, such as creating autorun entries for persistence.

- **Software Installation/Configuration:**

  It can be used to see what registry changes occur during software installation or configuration processes.

- **Troubleshooting:**

  If a program or system is behaving strangely, Regshot can help pinpoint registry changes that might be causing problems.

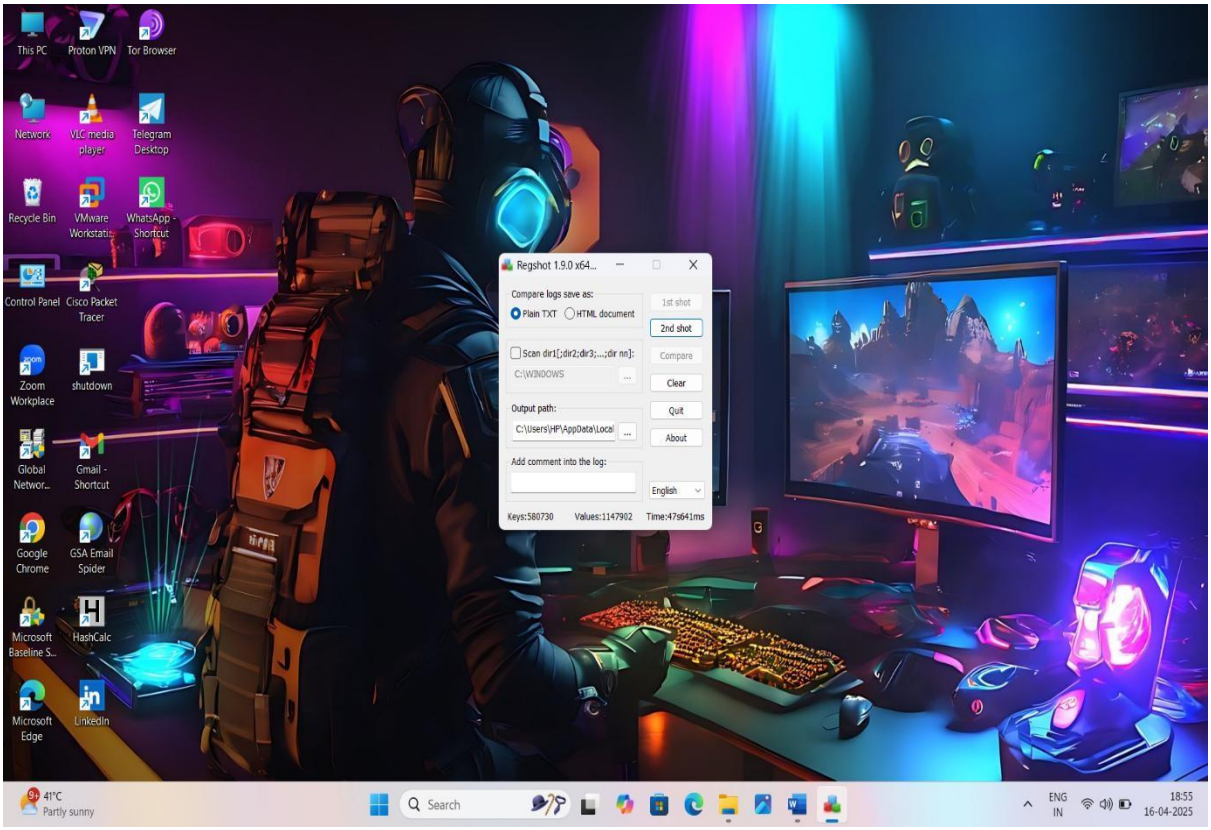
- **Dynamic Analysis:**

Name : kunal Jawale

Regshot is often used in conjunction with other tools like Process Monitor (ProcMon) to analyze the dynamic behavior of software and identify its interactions with the Windows registry.

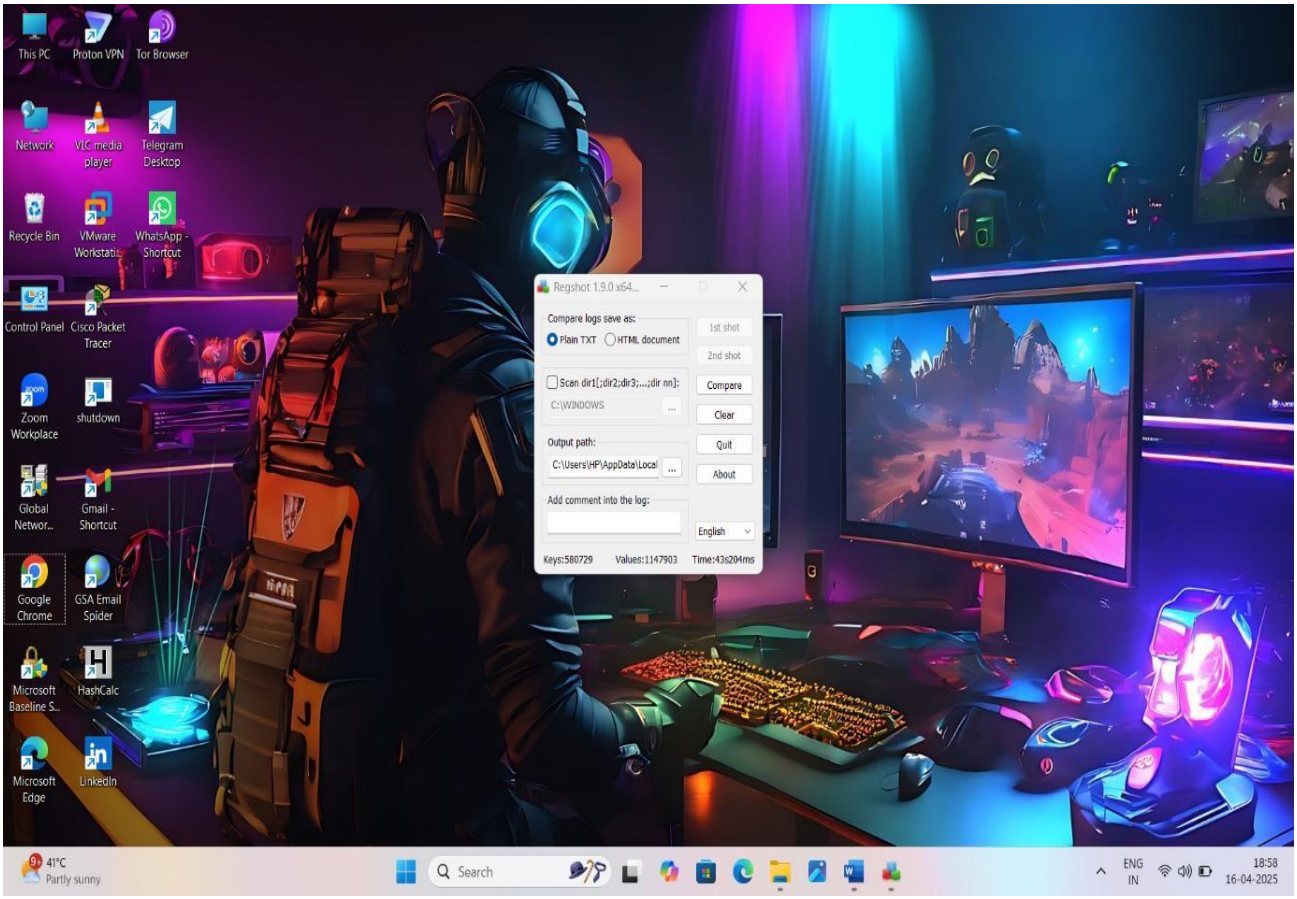
- **Registry Backup/Recovery:**
  Regshot can be used to create a baseline registry state before making significant changes, allowing for easy rollback if something goes wrong.

1st shot

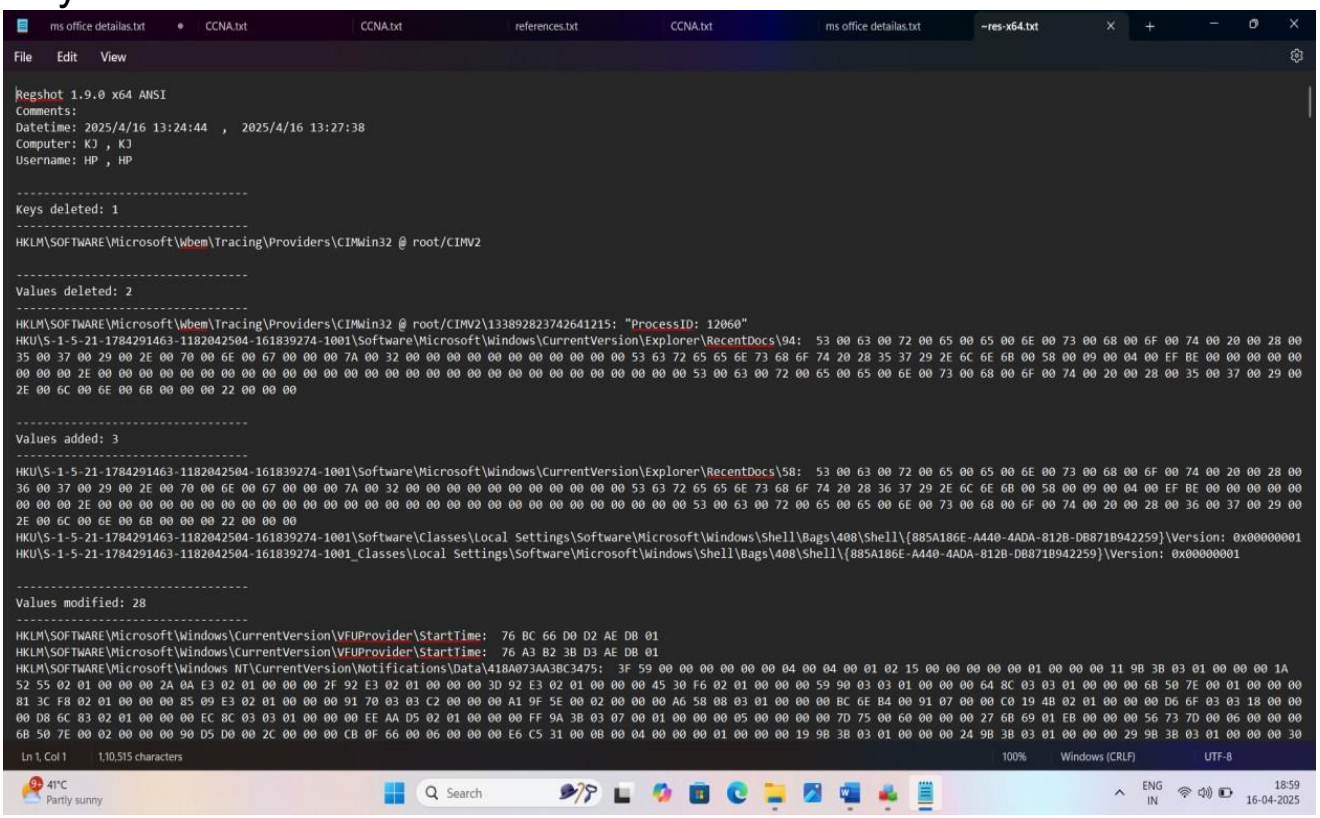


2nd shot

Name : kunal Jawale



And this is the comparison to show changes in values and which keys are added .



Name : kunal Jawale

O Tcpview :-

TCPView is a Windows tool used to display active TCP and UDP connections, including the processes using them. It can be used to monitor network activity, diagnose issues, and identify potential security risks by showing which applications are making connections to or from a server. It can also be used to close connections or kill processes from within the program.

- **Monitoring Network Activity:**

  TCPView allows users to see all active TCP and UDP connections on their system, including the local and remote IP addresses, ports, and connection state (e.g., "Listening," "Established").

- **Troubleshooting Network Problems:**

  By identifying the process associated with a specific network connection, users can troubleshoot issues like slow performance, unexpected network activity, or connection failures.

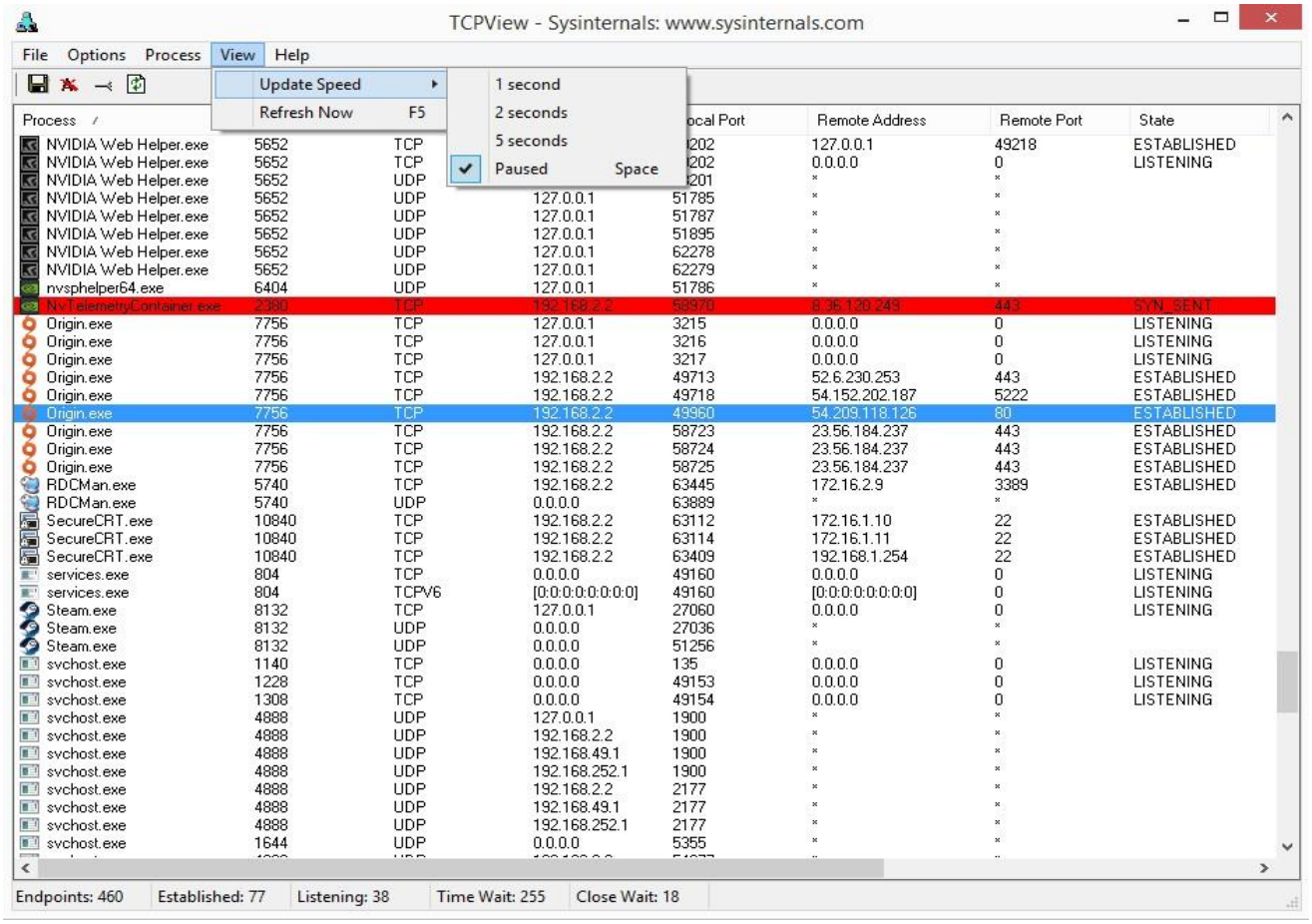
- **Identifying Suspicious Activity:**

  Security professionals can use TCPView to monitor for unusual outbound connections or processes using network resources, which could indicate malware or other malicious activity.

- **Closing Connections and Killing Processes:**

  TCPView allows users to close specific connections or kill the process associated with them, providing a way to manage network activity.

Name : kunal Jawale



➢ CURR port :-

CurrPorts is a Windows utility that displays all open TCP and UDP ports on a local computer, along with information about the processes using those ports. This tool helps identify which applications are connecting to and from the machine, aiding in troubleshooting and network security monitoring. It can also be used to close connections or kill processes associated with specific ports.

Here's a more detailed breakdown:

What it shows:

- **Open ports:**

  CurrPorts lists all currently open TCP and UDP ports on the system.

- **Associated processes:**

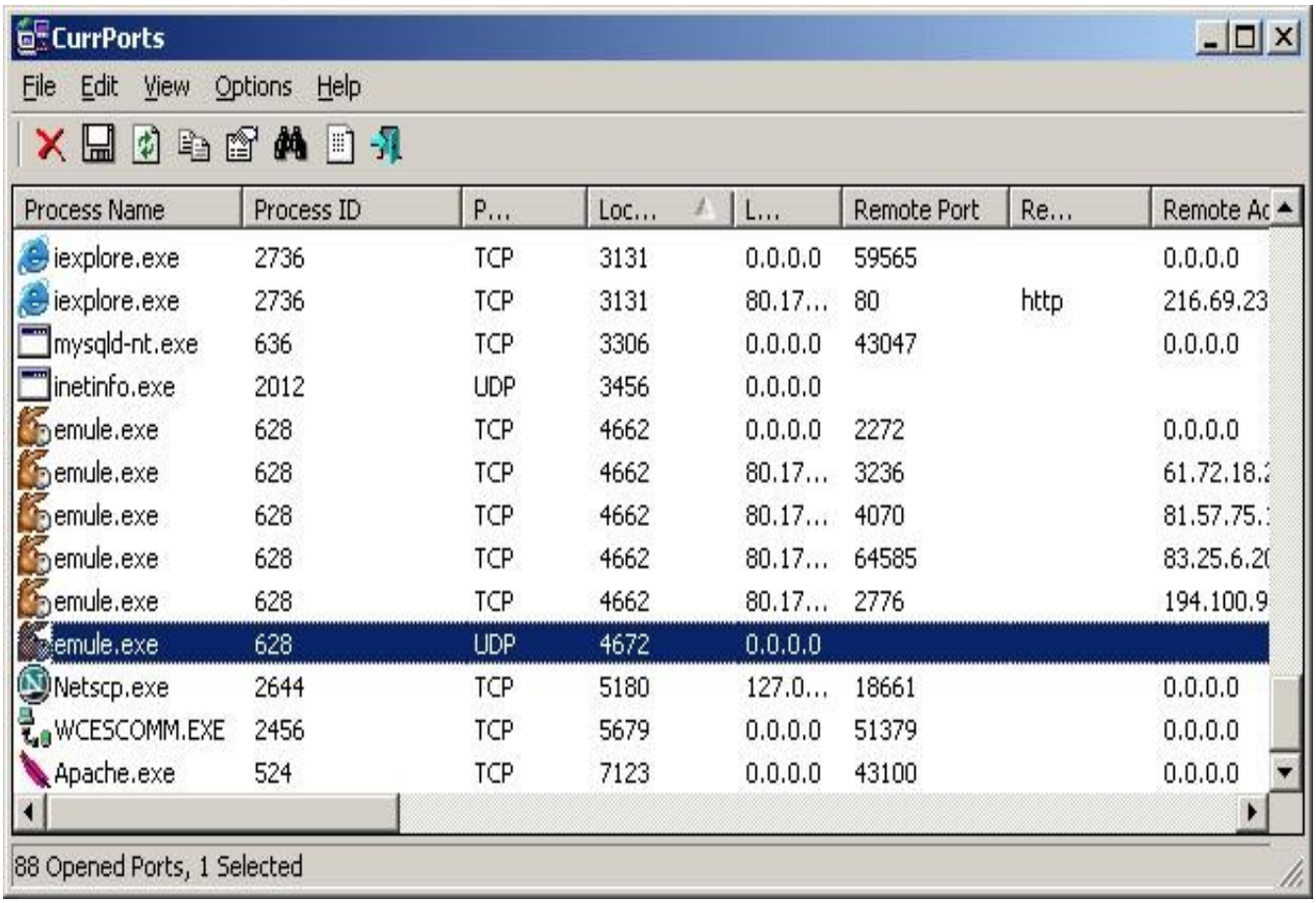
For each port, it displays the process that opened it, including the process name and full path.

- **Detailed information:**

  It provides information about the remote IP address, origin ports, destination ports, and open type for each connection.

- **Real-time updates:**

  CurrPorts can be configured to refresh the list automatically, allowing for realtime monitoring.



O Whats running :-

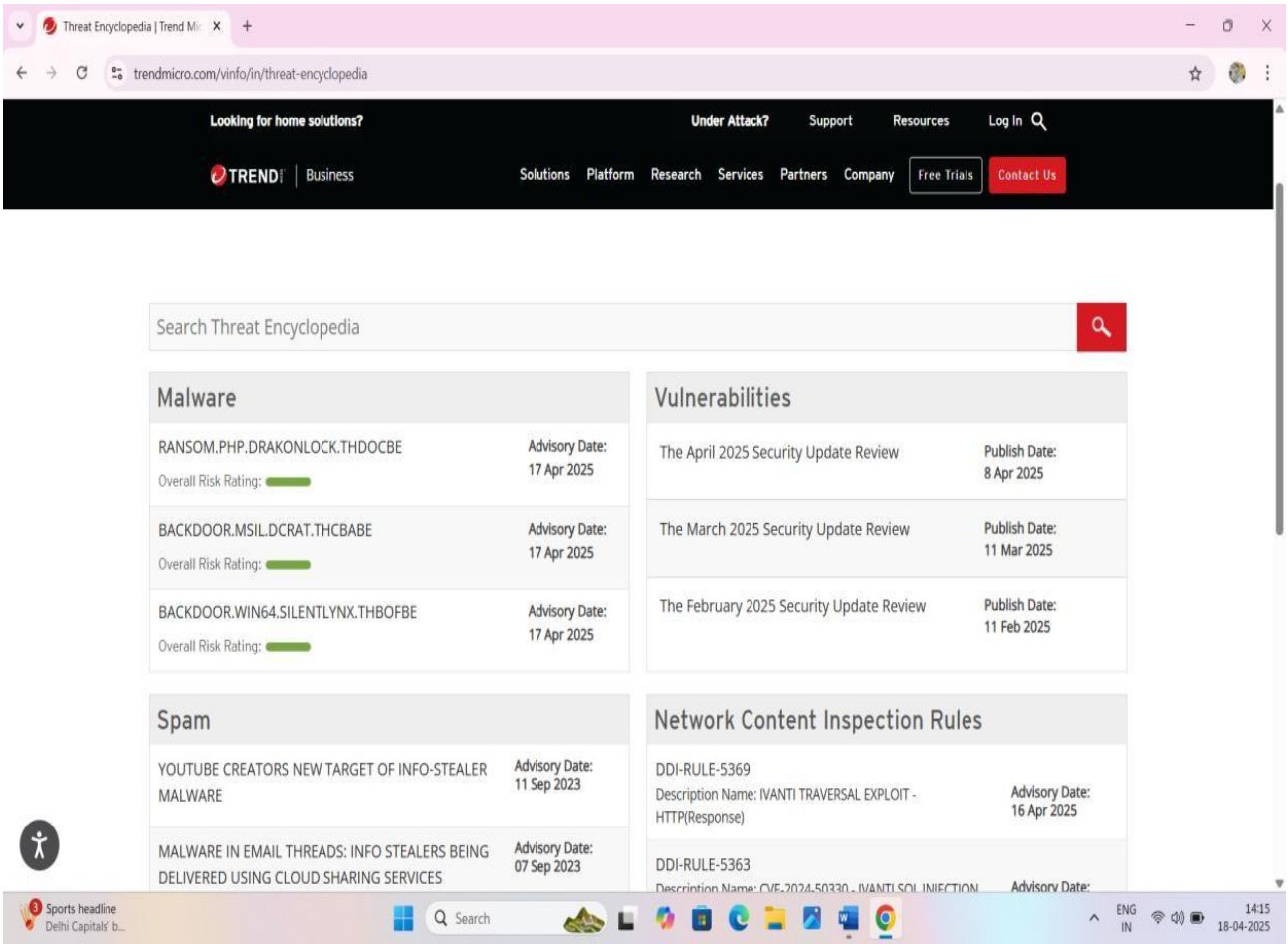
this app is same like curr ports and its useful for process and service monitoring and all types of monitoring

Name : kunal Jawale

/ here are one website for check latest malware and their information

o Latest malware encyclopedia

A "malware encyclopedia" is essentially a comprehensive database or resource that lists and describes different types of malicious software, including viruses, Trojans, ransomware, and more. It's a tool used by security researchers, organizations, and individuals to understand the threats they might face and how to defend against them.



Name : kunal Jawale