

# **Malware Behaviour Analysis and Windows Registry Investigation**

**Researching and analysing malware behaviour and  
its impact on the Windows Registry**

**CDAC, Noida**

**CYBER GYAN VIRTUAL  
INTERNSHIP PROGRAM**

**Submitted By:**

**Ankit ThakorBhai Gamit**

**Project Trainee, (May-June) 2024**

# BONAFIDE CERTIFICATE

This is to certify that this project report entitled **Malware Behaviour Analysis and Windows Registry Investigation** submitted to CDAC Noida, is a Bonafide record of work done by **Ankit ThakorBhai Gamit** under my supervision from **15<sup>TH</sup> May 2024 to 30<sup>TH</sup> June 2024**

(Signature)

HEAD OF THE DEPARTMENT

(Signature)

SUPERVISOR

## **Declaration by Author(s)**

This is to declare that this report has been written by me/us. No part of the report is plagiarized from other sources. All information included from other sources have been duly acknowledged. I/We aver that if any part of the report is found to be plagiarized, I/we are shall take full responsibility for it.

Name of Author(S): **Ankit ThakorBhai Gamit**

## **TABLE OF CONTENTS**

1.0 Introduction .....	06
1.1 Problem addressed.....	06
1.2 Learning objective .....	07
1.3 Approach .....	08
2.0 Implementation.....	09
2.1 Static Analysis .....	12
2.2 Dynamic Analysis.....	18
2.3 Windows Registry Investigation.....	23
3.0 Indicators Of Compromise(IOC) .....	28
4.0 Conclusion & Recommendations .....	29
5.0 List Of References .....	31

## ACKNOWLEDGEMENT

**I would like to thank all those who have supported me in the completion of the work, “Malware Behaviour Analysis and Windows Registry Investigation.” I would like to thank my supervisor, Varun Sir for the direction, support, and encouragement, which helped me in completing this research project, and for their deep knowledge and awareness of the cybersecurity. Without all of our mentors and their constant support and knowledge this project would not have been completed. I would like to thank CDAC for the opportunity, the resources, time, and a environment they have provided to perform the research, I am so grateful for their opportunity. Having the opportunity to use some advanced software and tools has been very helpful to me and my career and studies.**

# **Malware Behaviour Analysis and Windows Registry Investigation**

## **1.0**

### **Introduction**

The continuous rise of cybercrimes and usage of malware has brought an immense attention in cybersecurity since it currently poses a severe threat to humans, as well as to businesses. Malware actually is a malicious software which is used to harm or gain unauthorized access to personal information. Malware is basically designed to disrupt, damage, and or to gain unauthorized access to computer systems. Many malwares target the windows registry with respect to their goal of persistence, executing malicious payloads, as well as evading detection. This project is given to us to gain more knowledge about what the malware are doing in terms of behaviour and how they utilize Windows registry is very important in order to develop strong defense methods for counteracting and mitigating the potential threat.

## **1.1**

### **PROBLEM STATEMENT:**

#### **Malware Behaviour Analysis and Windows Registry Investigation**

### **PROBLEM ADDRESSED**

The identification and analysis of malware, even as new developments in cybersecurity are made, continues to be big problem, this is due to the constant evolution of tactics, techniques, and procedures, employed by Cyber criminals. One of the most common means for malware persistence and execution involves the Windows Registry. Due to the complexity involved in Windows Registry and the complex nature of current malware make it difficult to accurately detect and analyze these changes.

This project focuses on research and analysis of malware behaviour in respect to the Windows Registry. It will involve a deep study of various malware types, the mechanism of interaction with the Windows Registry, as well as implementation and evaluation of the analysis and investigation tools.

## 1.2

### **Learning Objective**

#### **1. Understanding Malware Behaviour**

- Types of Malware:

Training is received on various types of malware, such as viruses, worms Trojans, ransomware and spyware.

Different malware were viewed in their independent characteristics and advantages they use for an attack vector.

- Behaviour Patterns:

It has been observed try routine tactics, techniques and procedures common amongst malware in infecting systems

Documented how malware uses modification of the Windows Registry. Specific registry keys and values to look for that various malware strains target.

- IoCs

Registry Change IoC's, Recognised Run keys with unusual entries, shell commands changed and hidden services. Development methodology to look for while doing a malware investigation.

#### **2. Tool Proficiency Malware Analysis Tools:**

Earned experience for dynamic and static malware-sample analysis utilizing Cuckoo Sandbox.

Trained to use these normal tools to run malware samples in an isolated environment where I could observe the behaviour of a malware sample.

- Registry Monitoring Tools

Monitoring and recording registry changes using Regedit. Regshot to identify the various infected files and documents.

Trained in conducting a before and after snapshot of running malware to identify the changes introduced by malware. Forensic Analysis Tools.

#### **3. Analysis Techniques**

Static Analysis:

Static Analysis is the process by which analysis of malware binaries takes place without executing those binaries actually. Strings and proper indicators embedded in malware exposing its functionality have been recognized.

### Dynamic Analysis:

Behavioural analysis was carried out with the help of the Cuckoo Sandbox. Malware was dynamically analysed runtime; changes in file systems, network and registry have been observed

### Cross Method Comparison

The methods of static and dynamic analysis has been compared to observe malware

## 4. Documentation and Report

### Detailed Reporting

Malware analysis and its finding has properly been documented in a detailed report.

The report therefore includes information on identified IOCs, specific registry changes and overall malware behaviour

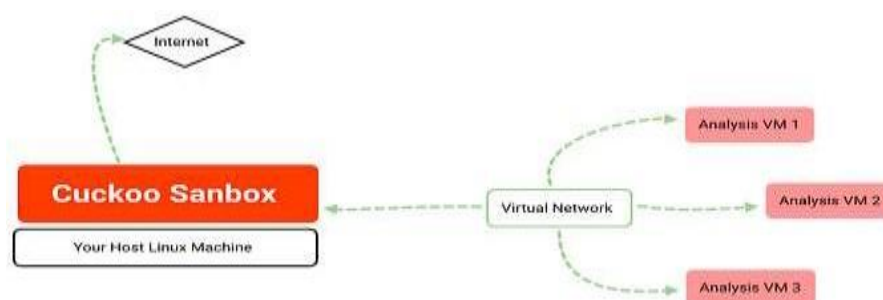
## 1.3

### APPROACH:

The tools and technologies that are used in this project are Oracle virtualbox version 7.0.10 , Cuckoo Sandbox version 2.0.7. I also used kali linux version 6.3.0 having IP address 10.0.2.15, Microsoft Windows [Version 10.0.22631.3737] with IP address 192.168.83.21. Technologies like python , MongoDB, swig and YARA are used for different purposes. Regedit and Regshot are used for Windows Registry Investigation.

In this project I used an approach in which the testing is done using Cuckoo Sandbox in the virtual box. The file containing virus is put in the cuckoo sandbox to analyse the file and generate the report. For that purpose I needed various software like python version 2.7 because the cuckoo sandbox is only compatible with Python of that version.

In this project the cuckoo sandbox is installed in the VM and the malware file is inserted in the cuckoo sandbox to analyze. After analysing the file Regedit is used for investigation in the windows registry .





## 2.0

### **IMPLEMENTATION:**

To Execute this project first setup an environment for the virtual machine to be installed.

#### ❖ **Choose a Virtualization Platform:**

Download and install VirtualBox or VMware Workstation Player.

#### ❖ **Create a New Virtual Machine:**

- Create a new VM.
- Download a Windows ISO and use it to install the OS on the VM.
- Set the network mode to Host-Only to isolate the VM.
- After the OS is installed and updated, create a snapshot for the virtual machine to be loaded for better security.



Download and install the following tools inside the VM

- ### ❖ Setup Cuckoo Sandbox:

- ```

kali@kali:~$ sudo apt-get install libnet16 libnetstring libncursesw libnet
virtualbox virtualbox-dm virtualbox-gt
The following packages will be upgraded:
gnutls-bin libe-bin libe-dev libe-devel libe-lib libe-libcdev
libe-libs libe-kernel locales openssl-client openssl-server
openssl-sftp-server openssl-pki-pki-pki-modules virtualbox-guest-utils
virtualbox-guest-vdi
18 upgraded, 0 newly installed, 0 to remove and 219 not upgraded.
Need to get 76.8 MB of archives.
After this operation, 187 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://mirror.kali.org/kali kali-rolling/main amd64 libe-bin amd64 2.10-10 [112 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libe-lib all 2.10-10 [72 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 libe-devel amd64 2.10-10 [57.3 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 libe-dev amd64 2.10-10 [46.5 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 libe-libs amd64 2.10-10 [2,473 kB]
Get:6 http://mirror.freemf.org/kali kali-rolling/main amd64 gnutls-bin amd64 3.8.5-2 [470 kB]
Get:7 http://mirror.mkn.org/kali kali-rolling/main amd64 locales all 2.10-10 [2,912 kB]
Get:8 http://mirrors.uswest.edu.cn/kali kali-rolling/main amd64 libe-dev amd64 2.10-10 [1,954 kB]
Get:9 http://mirror.freemf.org/kali kali-rolling/main amd64 openssl-server amd64 1.9.7j-5 [450 kB]
Get:10 http://http.kali.org/kali kali-rolling/contrib amd64 virtualbox-gt amd64 7.0.14-frog-140 [24.7 MB]
Get:11 http://mirrors.uswest.edu.cn/kali kali-rolling/main amd64 libgnutls-deb04 amd64 3.8.5-2 [435 kB]
Get:12 http://mirrors.uswest.edu.cn/kali kali-rolling/main amd64 pki-kit amd64 0.25.3-5 [106 kB]
Get:13 http://http.kali.org/kali kali-rolling/contrib amd64 virtualbox-guest-vdi amd64 7.0.14-frog-140 [277 kB]
Get:14 http://kali.download/kali kali-rolling/main amd64 libe-libs amd64 2.10-10 [2,473 kB]
Get:15 http://kali.download/kali kali-rolling/main amd64 libnet16 amd64 3.9.1-2.2 [190 kB]
Get:16 http://kali.download/kali kali-rolling/main amd64 libnetstring amd64 3.9.1-2.2 [110 kB]
Get:17 http://kali.download/kali kali-rolling/main amd64 pki-modules amd64 0.25.3-5 [273 kB]
Get:18 http://kali.download/kali kali-rolling/main amd64 libe-kernel amd64 0.25.3-5 [415 kB]
Get:19 http://kali.download/kali kali-rolling/main amd64 libnetstrings amd64 3.9.1-2 [425 kB]
Get:20 http://kali.download/kali kali-rolling/main amd64 libnetstring amd64 3.9.1-2 [425 kB]
Get:21 http://kali.download/kali kali-rolling/main amd64 openssl-sftp-server amd64 1.9.7j-5 [453 kB]
Get:22 http://kali.download/kali kali-rolling/main amd64 openssl-client amd64 1.9.7j-5 [453 kB]
Get:23 http://kali.download/kali kali-rolling/main amd64 openssl-pki-pki-modules amd64 0.25.3-5 [2,244 kB]
Get:24 http://kali.download/kali kali-rolling/main amd64 dmz all 3.8.10-1 [21.6 kB]
Get:25 http://http.kali.org/kali kali-rolling/main amd64 libnet-3.8.10-1 amd64 3.8.10-1 [290 kB]
Get:26 http://http.kali.org/kali kali-rolling/main amd64 libnet amd64 3.9.1-2.2 [190 kB]
Get:27 http://http.kali.org/kali kali-rolling/main amd64 libncursesw amd64 6.4+20191012 [262 kB]
Get:28 http://http.kali.org/kali kali-rolling/contrib amd64 virtualbox-dm amd64 7.0.14-frog-140 [700 kB]
Get:29 http://http.kali.org/kali kali-rolling/contrib amd64 virtualbox amd64 7.0.14-frog-140 [25.4 MB]
Get:30 http://http.kali.org/kali kali-rolling/contrib amd64 virtualbox-guest-utils amd64 7.0.14-frog-140 [400 kB]
Get:31 http://kali.download/kali kali-rolling/main amd64 libe-libs amd64 2.10-10 [2,473 kB]
Fetched 75.3 MB in 44s (1,695 KB/s)

```

```

Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Jun 9 08:12

ankit@Ankit: ~
Is the information correct? [Y/n] Y
info: Adding new user 'cuckoo' to supplemental / extra groups 'users' ...
info: Adding user 'cuckoo' to group 'users' ...

(ankit@Ankit)~[~]
$ sudo usermod -a -G vboxusers cuckoo

(ankit@Ankit)~[~]
$ sudo usermod -a -G libvirt cuckoo
usermod: group 'libvirt' does not exist

(ankit@Ankit)~[~]
$ sudo pip install -U pip setuptools
Requirement already satisfied: pip in /usr/lib/python3/dist-packages (23.2)
Collecting pip
  Obtaining dependency information for pip from https://files.pythonhosted.org/packages/ba/ba/19e9fe04fca059ccf770861c7d5721ab4c2aebc539889e97c7977528a53b/pip-24.0-py3-none-any.whl.metadata
  Downloading pip-24.0-py3-none-any.whl.metadata (3.6 kB)
Requirement already satisfied: setuptools in /usr/lib/python3/dist-packages (67.8.0)
Collecting setuptools
  Obtaining dependency information for setuptools from https://files.pythonhosted.org/packages/de/88/70c5767a0e43eb4451c220f07d042a4bcd7639276003a9c54a68cfcc1f8/setuptools-70.0.0-py3-none-any.whl.metadata
  Using cached setuptools-70.0.0-py3-none-any.whl.metadata (5.9 kB)
  Downloading pip-24.0-py3-none-any.whl (2.1 MB)
2.1/2.1 MB 3.0 MB/s eta 0:00:00
Using cached setuptools-70.0.0-py3-none-any.whl (863 kB)
Installing collected packages: setuptools, pip
  Attempting uninstall: setuptools
    Found existing installation: setuptools 67.8.0
    Not uninstalling setuptools at /usr/lib/python3/dist-packages, outside environment /usr
    Can't uninstall 'setuptools'. No files were found to uninstall.
  Attempting uninstall: pip
    Found existing installation: pip 23.2
    Not uninstalling pip at /usr/lib/python3/dist-packages, outside environment /usr
    Can't uninstall 'pip'. No files were found to uninstall.
Successfully installed pip-24.0 setuptools-70.0.0
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv

(ankit@Ankit)~[~]
$

```

```

Windows 10 (x64) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Jun 9 08:12

ankit@Ankit: ~
Is the information correct? [Y/n] Y
info: Adding new user 'cuckoo' to supplemental / extra groups 'users' ...
info: Adding user 'cuckoo' to group 'users' ...

(ankit@Ankit)~[~]
$ sudo usermod -a -G vboxusers cuckoo

(ankit@Ankit)~[~]
$ sudo usermod -a -G libvirt cuckoo
usermod: group 'libvirt' does not exist

(ankit@Ankit)~[~]
$ sudo pip install -U pip setuptools
Requirement already satisfied: pip in /usr/lib/python3/dist-packages (23.2)
Collecting pip
  Obtaining dependency information for pip from https://files.pythonhosted.org/packages/ba/ba/19e9fe04fca059ccf770861c7d5721ab4c2aebc539889e97c7977528a53b/pip-24.0-py3-none-any.whl.metadata
  Downloading pip-24.0-py3-none-any.whl.metadata (3.6 kB)
Requirement already satisfied: setuptools in /usr/lib/python3/dist-packages (67.8.0)
Collecting setuptools
  Obtaining dependency information for setuptools from https://files.pythonhosted.org/packages/de/88/70c5767a0e43eb4451c220f07d042a4bcd7639276003a9c54a68cfcc1f8/setuptools-70.0.0-py3-none-any.whl.metadata
  Using cached setuptools-70.0.0-py3-none-any.whl.metadata (5.9 kB)
  Downloading pip-24.0-py3-none-any.whl (2.1 MB)
2.1/2.1 MB 3.0 MB/s eta 0:00:00
Using cached setuptools-70.0.0-py3-none-any.whl (863 kB)
Installing collected packages: setuptools, pip
  Attempting uninstall: setuptools
    Found existing installation: setuptools 67.8.0
    Not uninstalling setuptools at /usr/lib/python3/dist-packages, outside environment /usr
    Can't uninstall 'setuptools'. No files were found to uninstall.
  Attempting uninstall: pip
    Found existing installation: pip 23.2
    Not uninstalling pip at /usr/lib/python3/dist-packages, outside environment /usr
    Can't uninstall 'pip'. No files were found to uninstall.
Successfully installed pip-24.0 setuptools-70.0.0
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv

(ankit@Ankit)~[~]
$

```

## 2.1

### Static Analysis

#### Step 1: Initial Examination

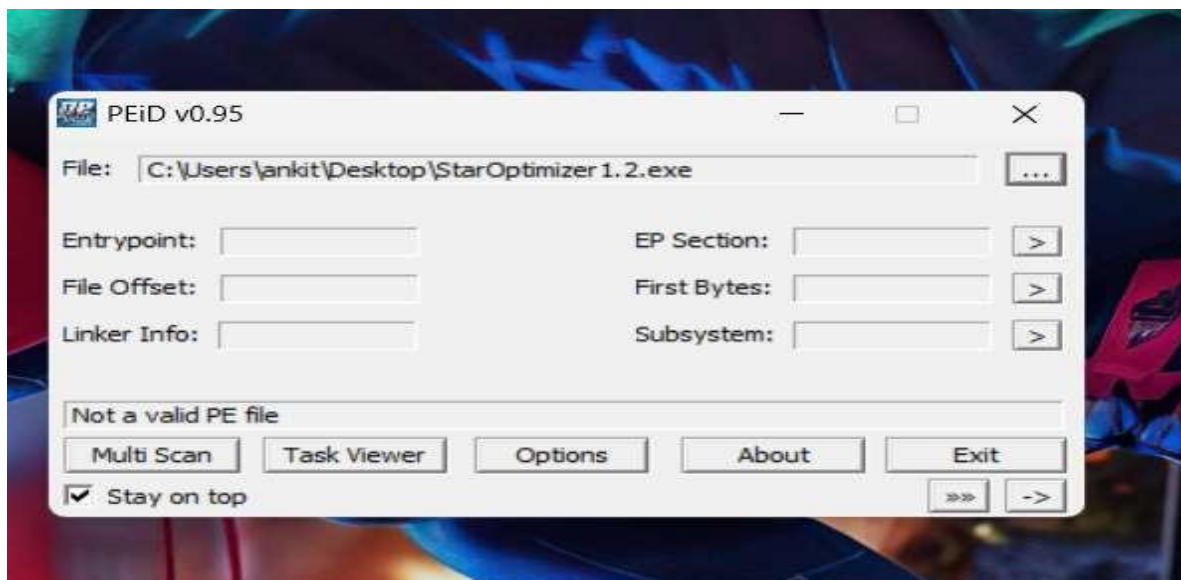
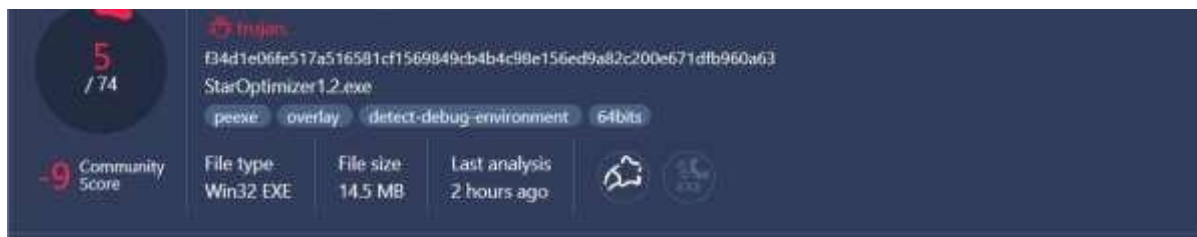
##### 1. File Headers:

- Use PEiD to inspect file headers.
- Document file type, size, and attributes.

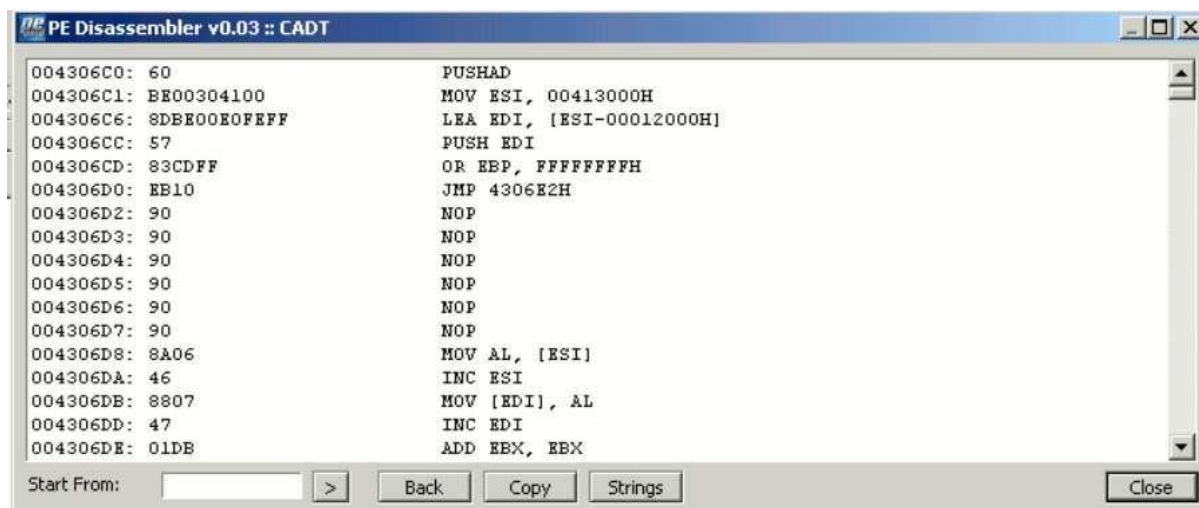
The file that I selected is .exe file that is a trojan malware. I downloaded this file from <https://malshare.com>.

As seen the below image the file type is Win32 EXE. The size of the file is 14.5 MB. Its various attributes are displayed in the image.

The name of this file is “f34d1e06fe517a516581cf1569849cb4b4c98e156ed9a82c200e671dfb960a63” and StarOptimizer1.2.exe.



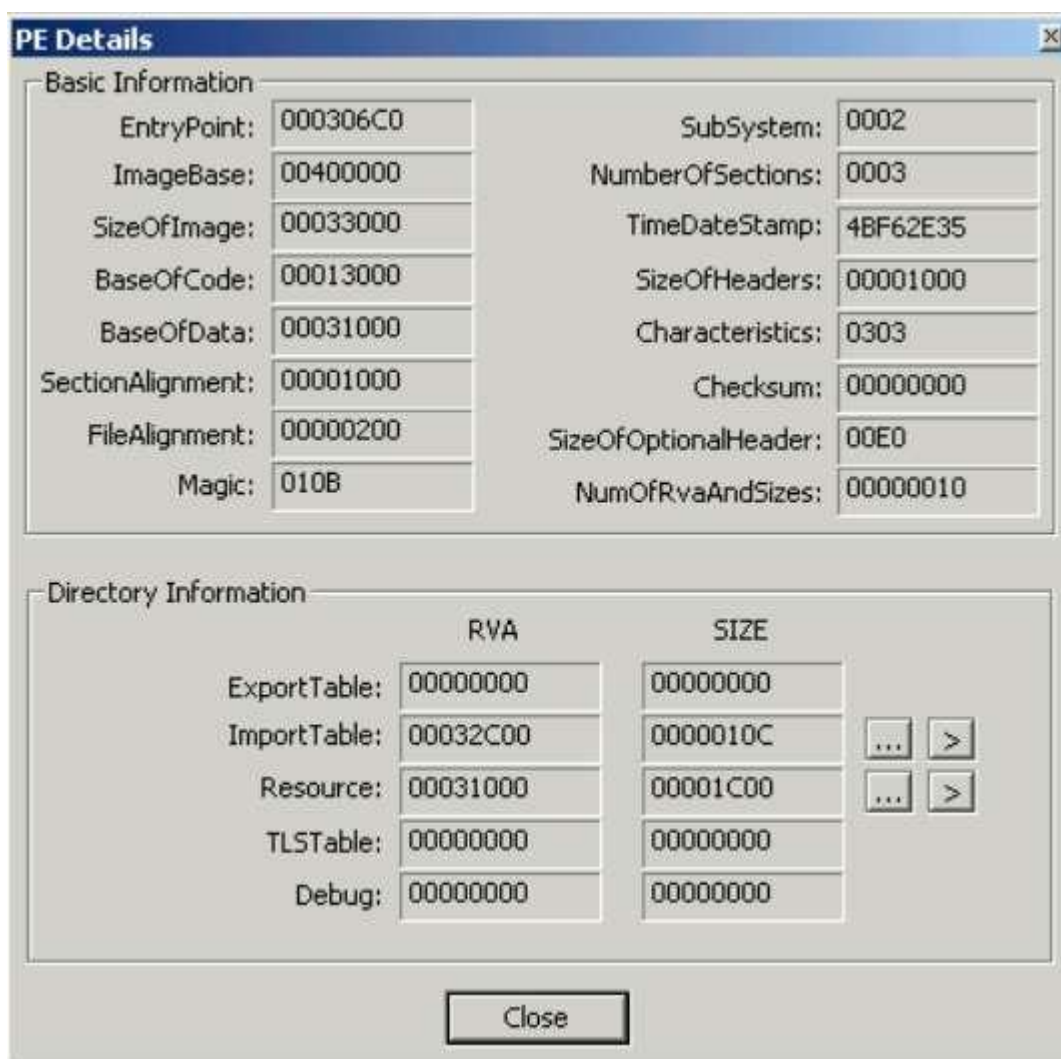




PE Disassembler v0.03 :: CADT

| Address                | Disassembly              |
|------------------------|--------------------------|
| 004306C0: 60           | PUSHAD                   |
| 004306C1: BE00304100   | MOV ESI, 00413000H       |
| 004306C6: 8DBE00E0FEFF | LEA EDI, [ESI-00012000H] |
| 004306CC: 57           | PUSH EDI                 |
| 004306CD: 83CDFF       | OR EBP, FFFFFFFFH        |
| 004306D0: EB10         | JMP 4306E2H              |
| 004306D2: 90           | NOP                      |
| 004306D3: 90           | NOP                      |
| 004306D4: 90           | NOP                      |
| 004306D5: 90           | NOP                      |
| 004306D6: 90           | NOP                      |
| 004306D7: 90           | NOP                      |
| 004306D8: 8A06         | MOV AL, [ESI]            |
| 004306DA: 46           | INC ESI                  |
| 004306DB: 8B07         | MOV [EDI], AL            |
| 004306DD: 47           | INC EDI                  |
| 004306DE: 01DB         | ADD EBX, EBX             |

Start From:  > Back Copy Strings Close



PE Details

Basic Information

|                   |          |                       |          |
|-------------------|----------|-----------------------|----------|
| EntryPoint:       | 000306C0 | SubSystem:            | 0002     |
| ImageBase:        | 00400000 | NumberOfSections:     | 0003     |
| SizeOfImage:      | 00033000 | TimeDateStamp:        | 4BF62E35 |
| BaseOfCode:       | 00013000 | SizeOfHeaders:        | 00001000 |
| BaseOfData:       | 00031000 | Characteristics:      | 0303     |
| SectionAlignment: | 00001000 | Checksum:             | 00000000 |
| FileAlignment:    | 00000200 | SizeOfOptionalHeader: | 00E0     |
| Magic:            | 010B     | NumOfRvaAndSizes:     | 00000010 |

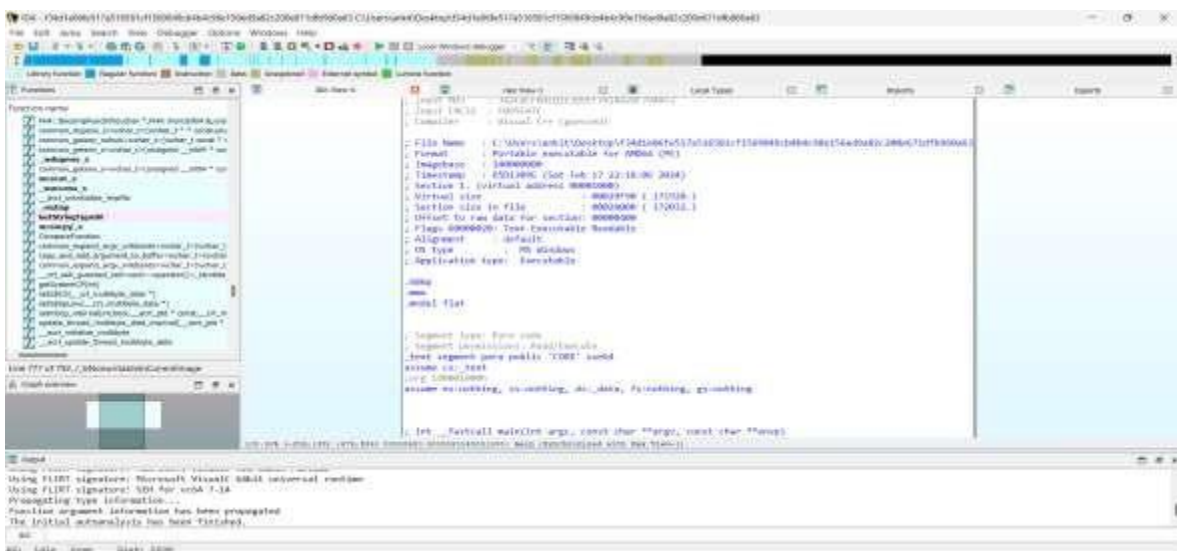
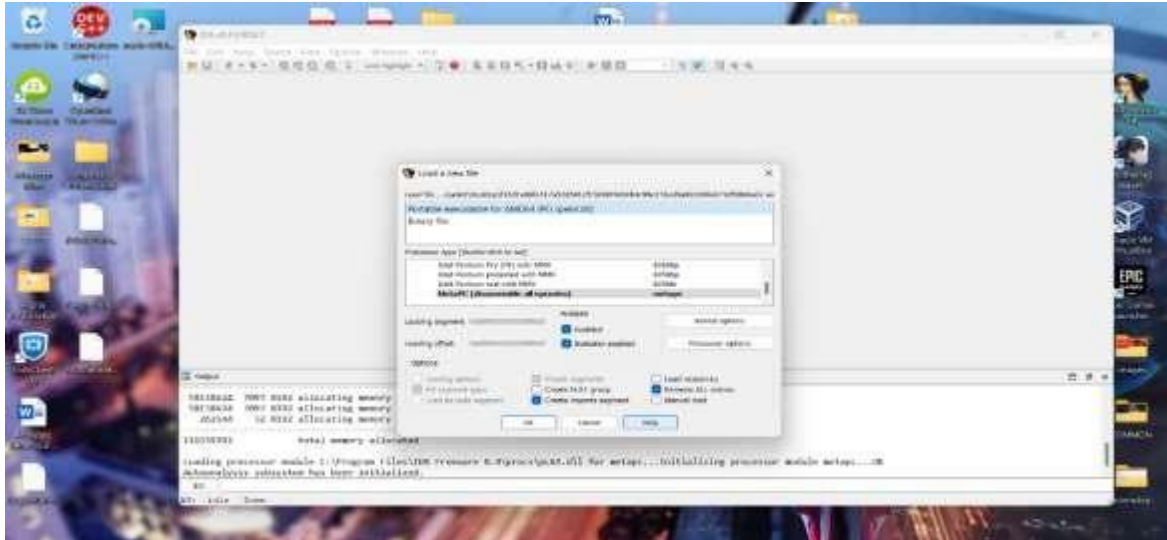
Directory Information

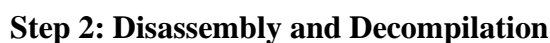
|              | RVA      | SIZE     |     |
|--------------|----------|----------|-----|
| ExportTable: | 00000000 | 00000000 |     |
| ImportTable: | 00032C00 | 0000010C | ... |
| Resource:    | 00031000 | 00001C00 | ... |
| TLSTable:    | 00000000 | 00000000 |     |
| Debug:       | 00000000 | 00000000 |     |

Close

## 2. Strings Extraction:

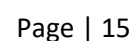
- Use strings command or tools like IDA to extract strings.
- Look for URLs, file paths, and registry keys.

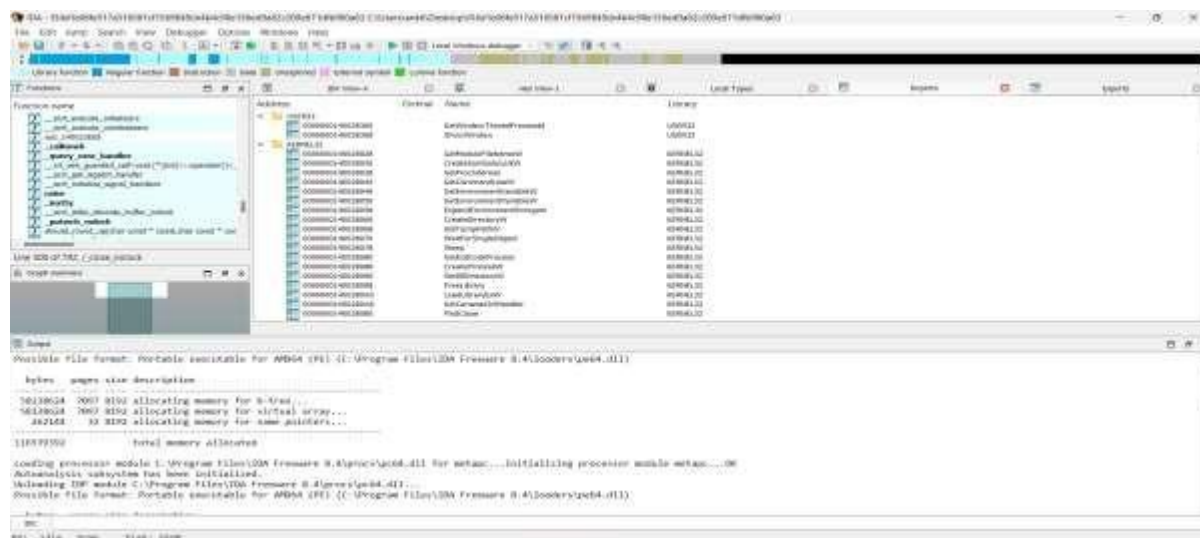




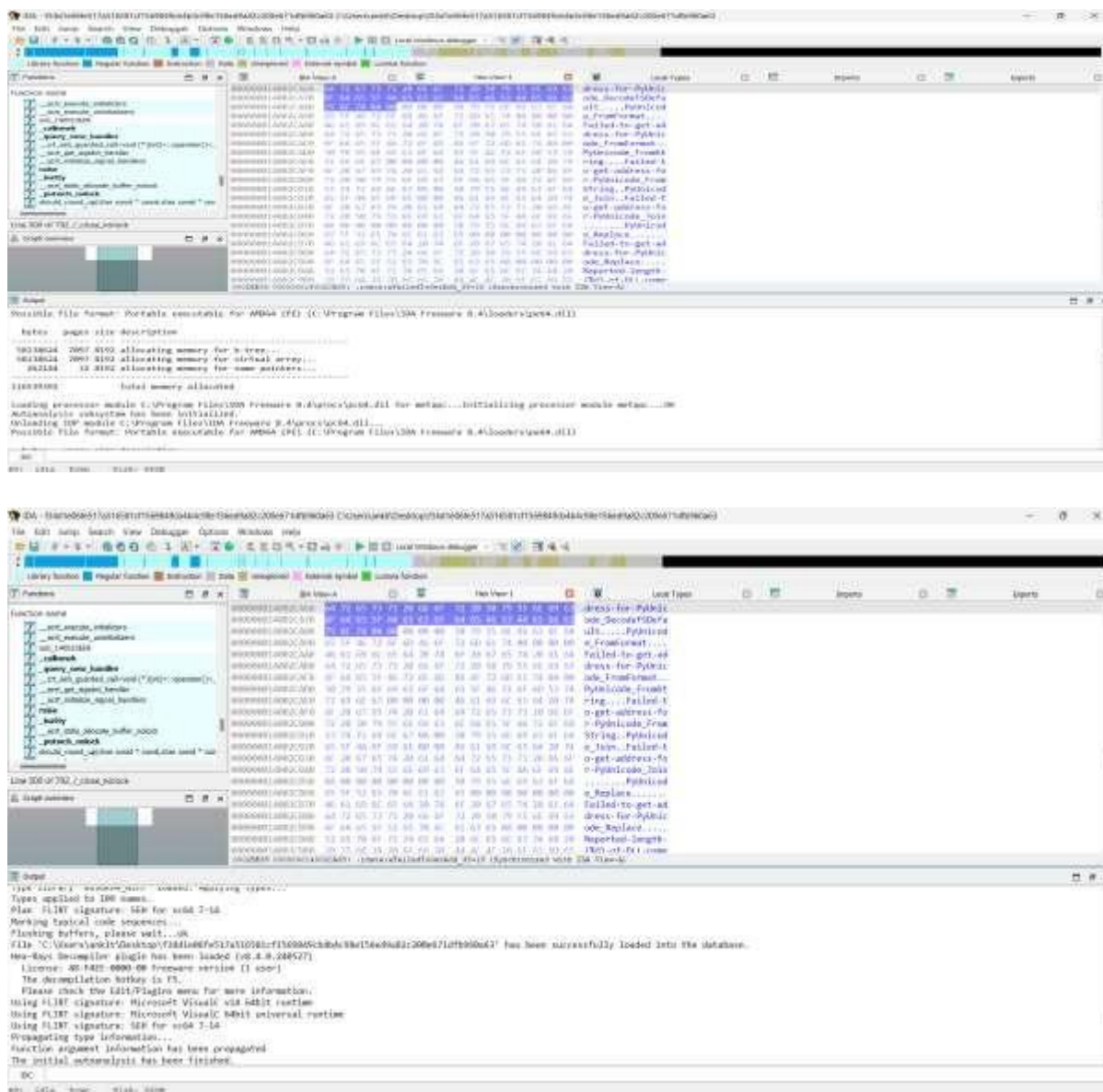
- Load the malware in IDA or any other tool.
- Let the tool analyze and disassemble the binary.

- Identify key functions and API calls.
- Document control flow and suspicious functions.







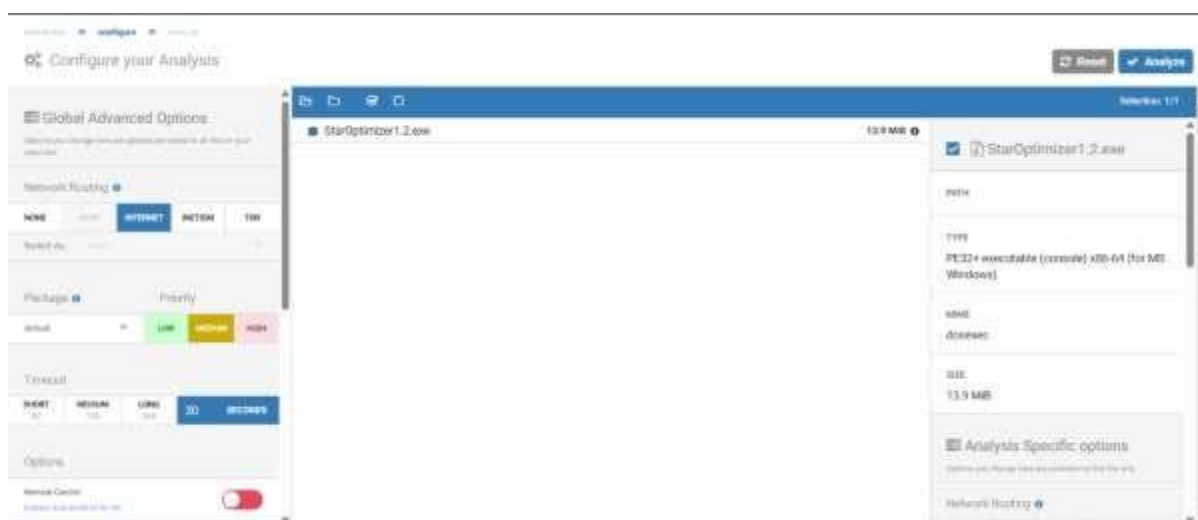
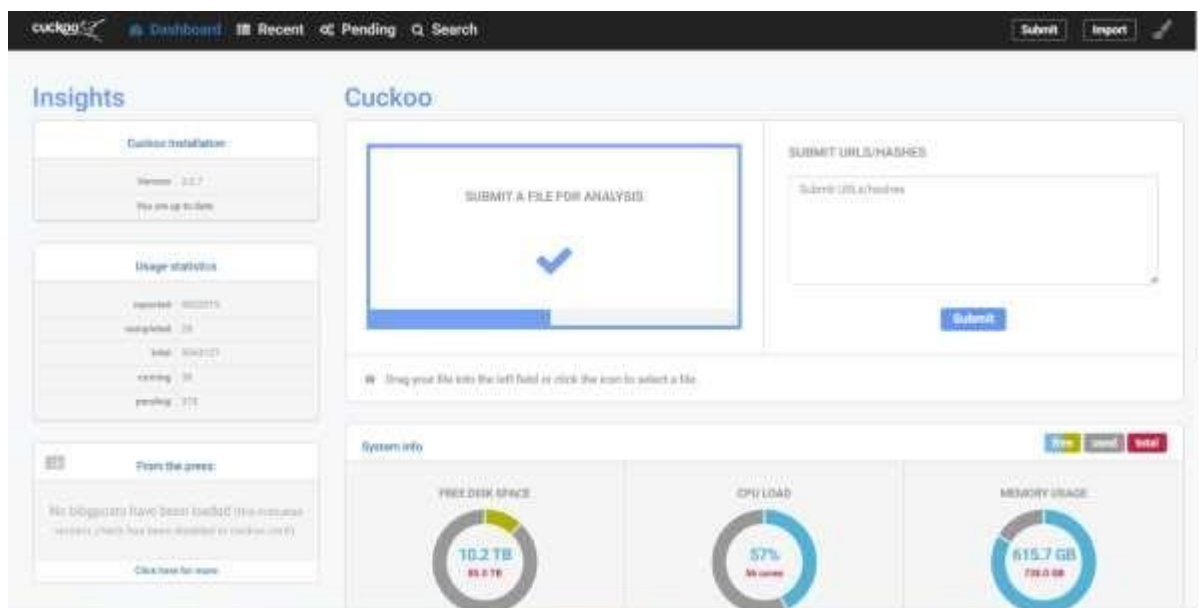


## 2.2

### Dynamic Analysis

#### Step 1: Preparing the Sandbox

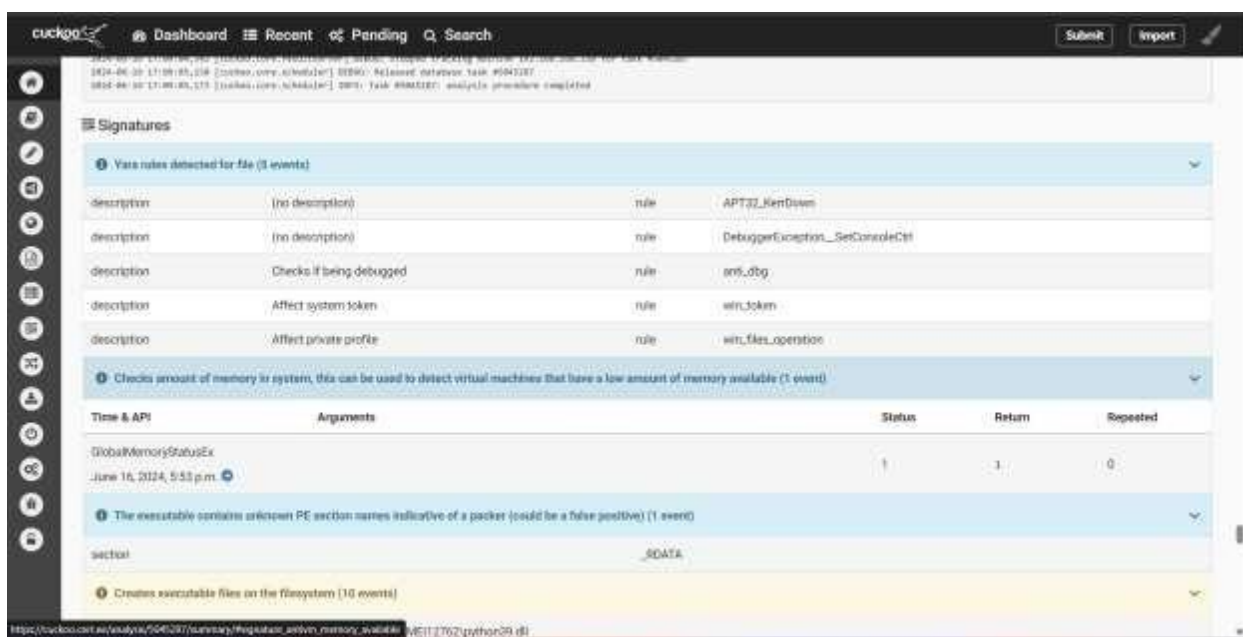
1. **Snapshot:** Take a snapshot of the clean VM state.
2. **Run Malware in Cuckoo:**
  - Submit the malware to Cuckoo Sandbox.
  - Monitor through Cuckoo's web interface.



[illegible]



This is the image of the file that popping when the file is executed.







[illegible]

Page | 22

## 2.3

### Windows Registry Investigation

#### Step 1

1. **RegShot:**

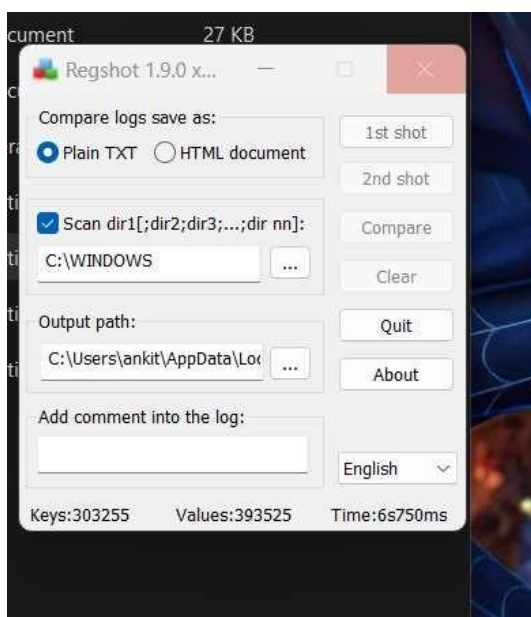
- Take an initial snapshot of the registry.
- Run the malware and take a second snapshot.
- Compare the snapshots for changes.

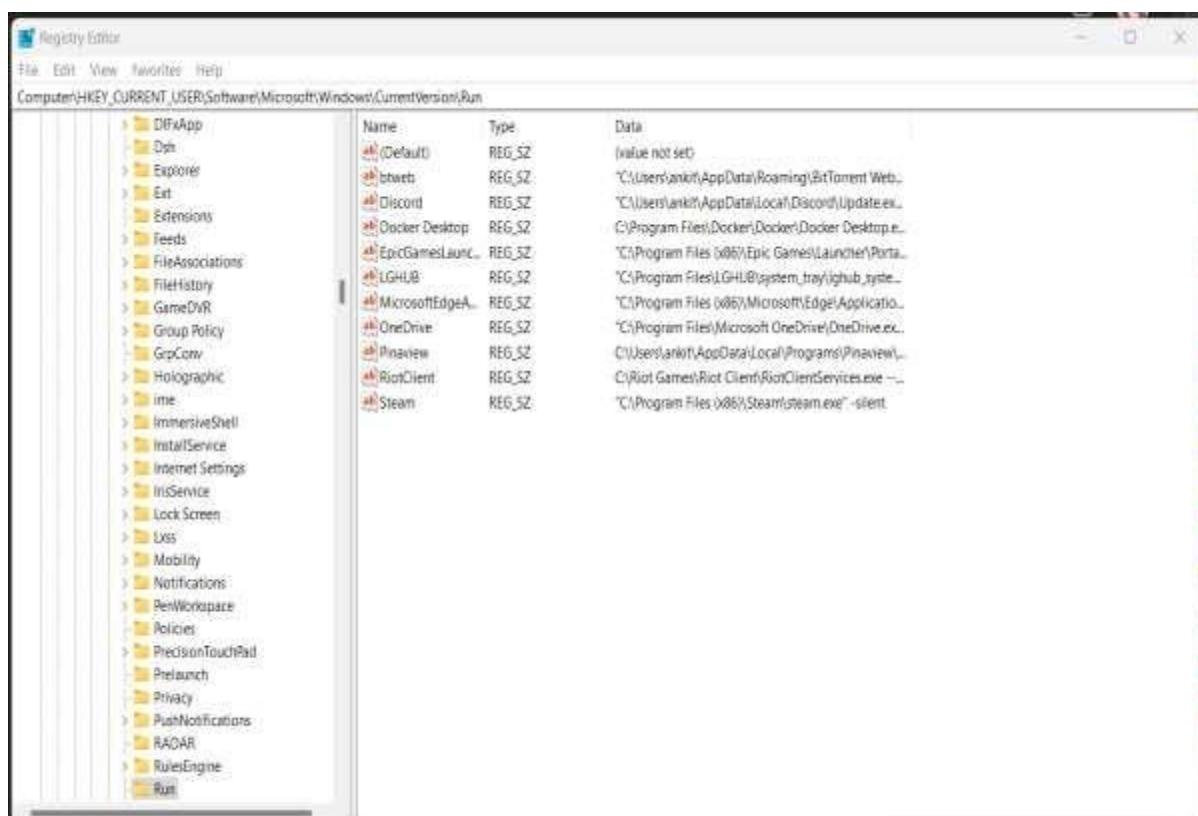
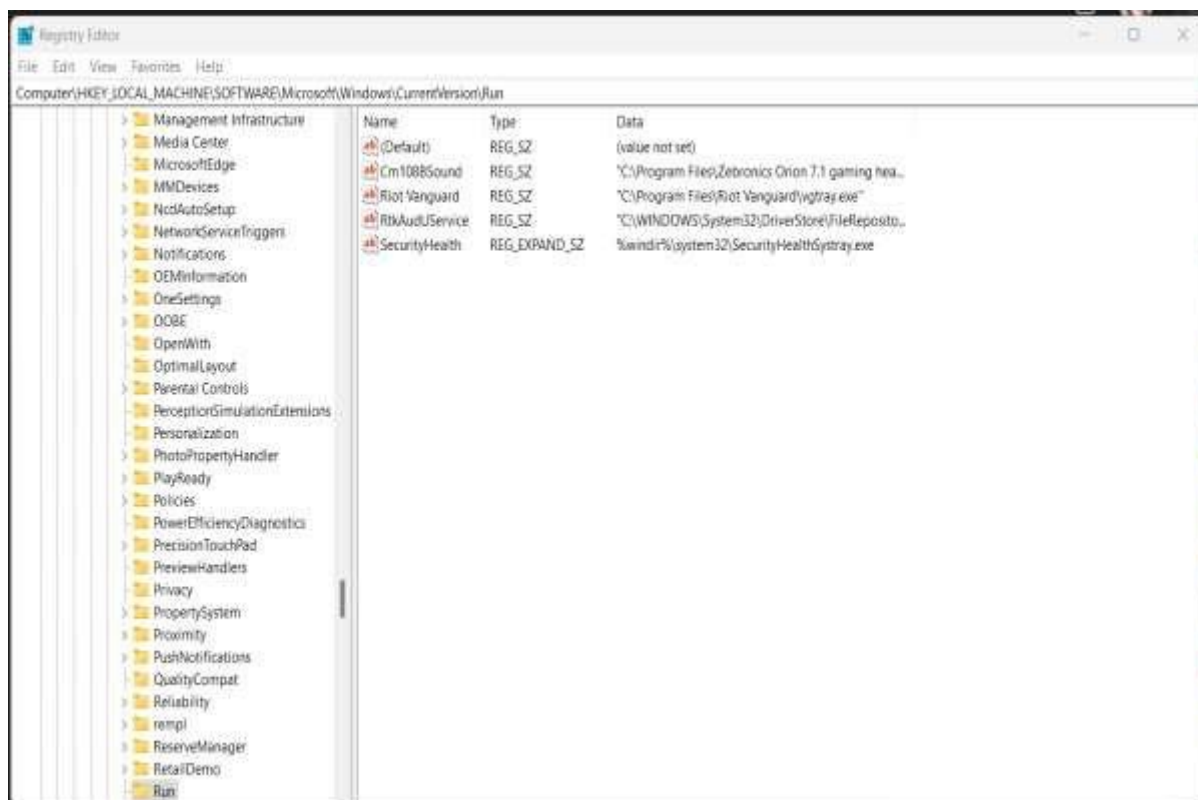
2. **Regedit:**

- Use regedit to see the file changes made in any directory.

3. **Wireshark:**

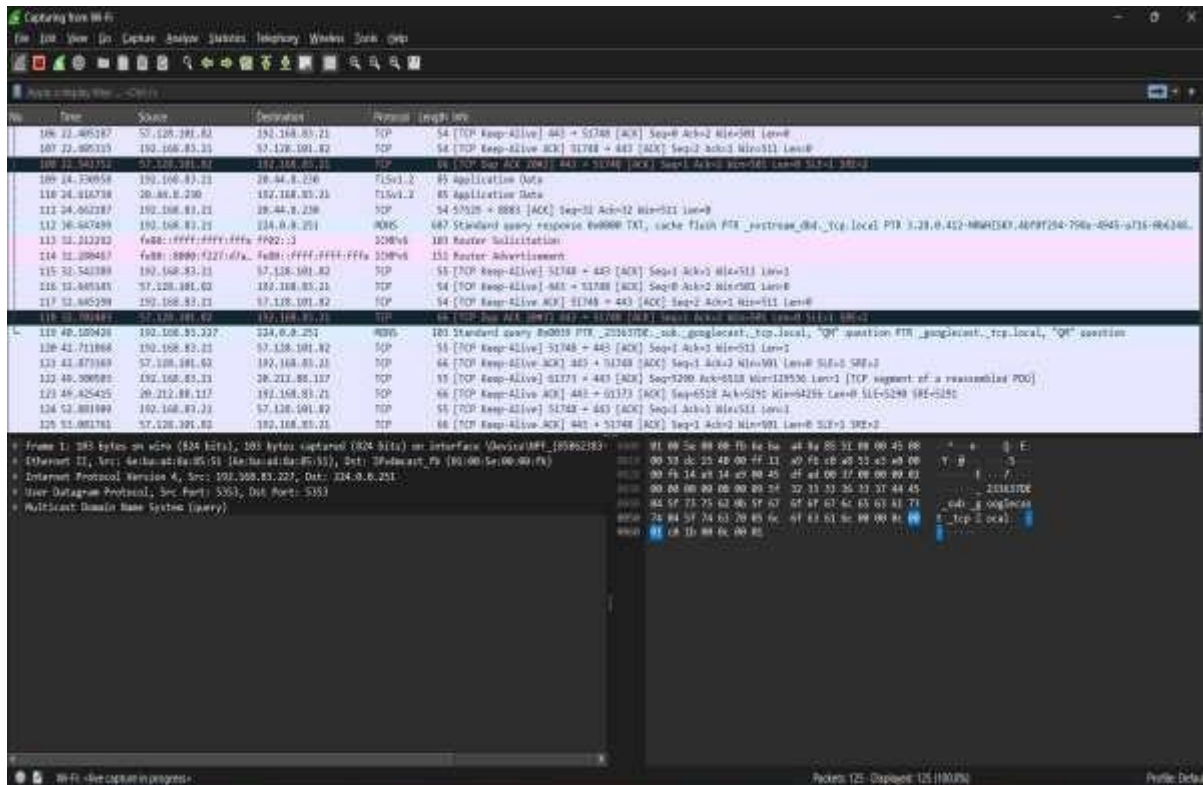
- Start capturing network traffic before running the malware.







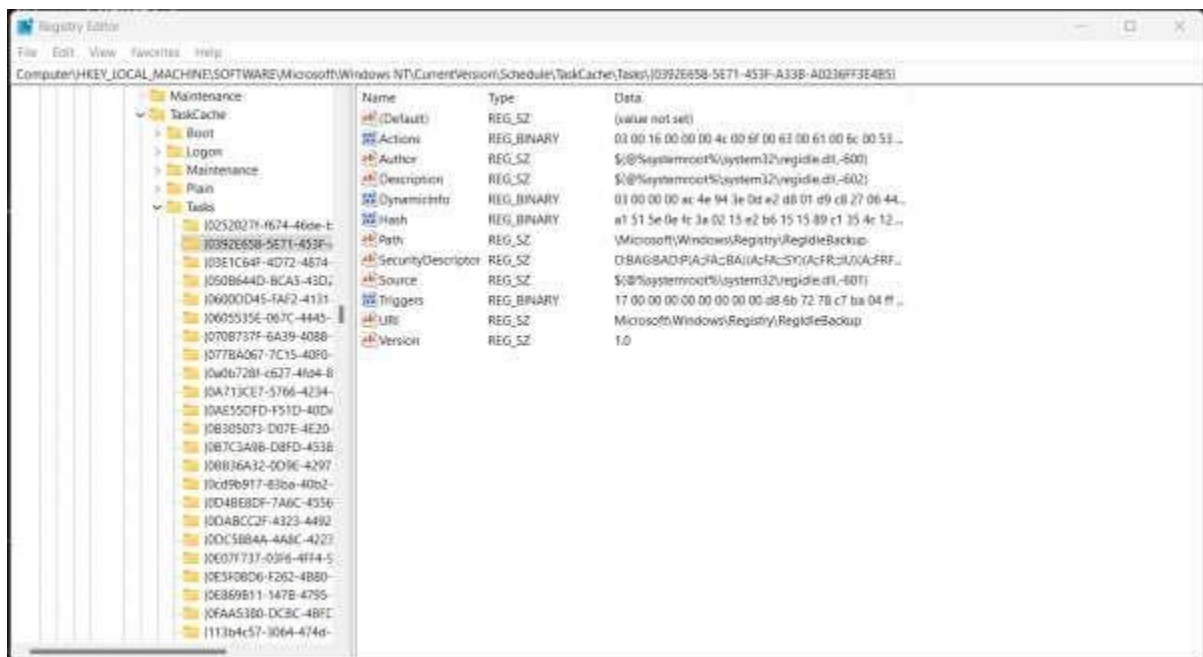




## Step 2: Document Observations

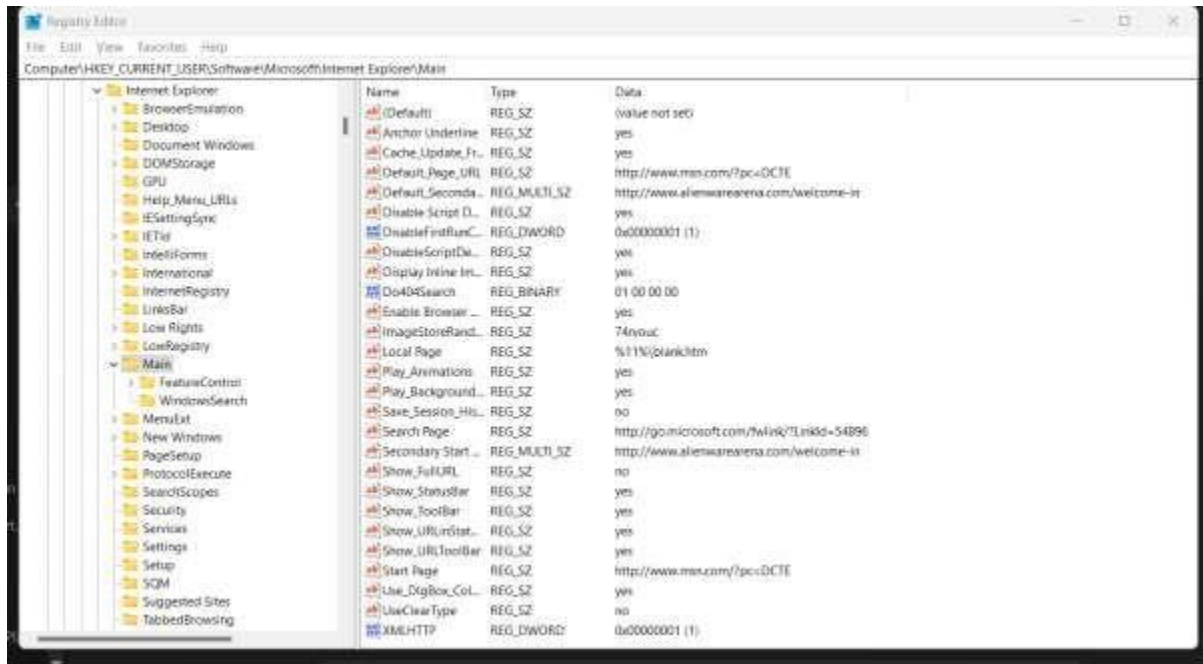
### 1. File System Changes:

- Note new, modified, or deleted files.



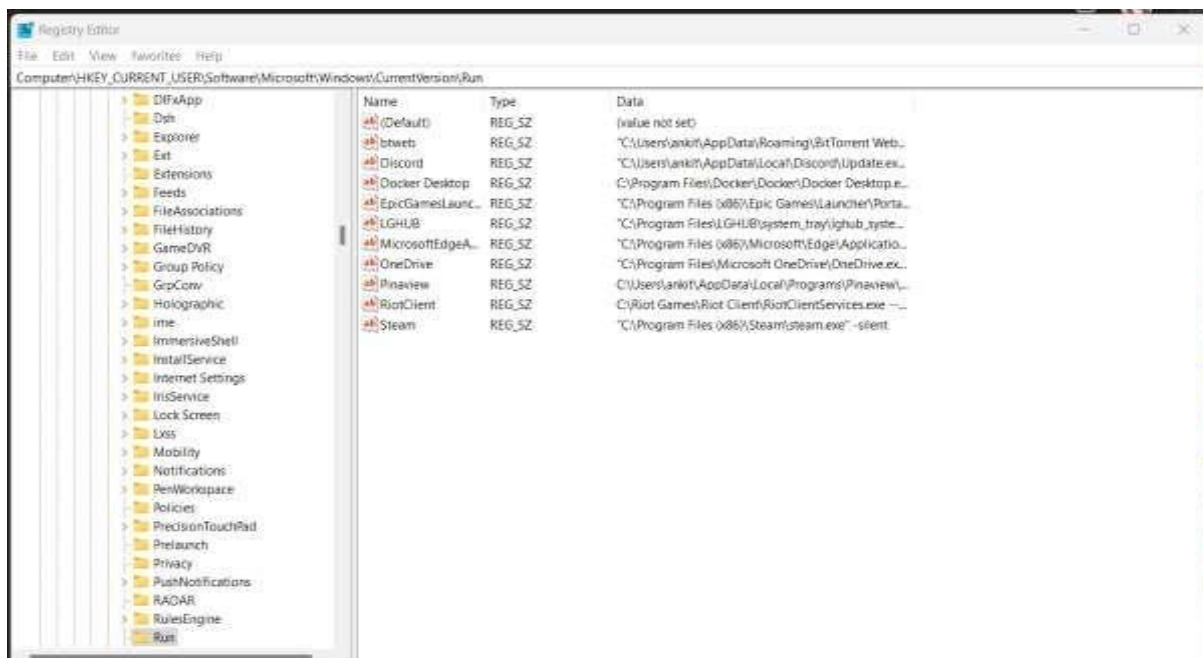
## 2. Network Activity:

- Document connections to external IP addresses.



## 3. Registry Modifications:

- Record changes, especially in autostart locations.



After Performing all the needed steps, see if there is any change in files of your Device.

### 3.0

**Indicators Of Compromise(IOC):** After the attack was performed I noticed several IOC's such as

- As I executed the Malware I noticed Calls to suspicious API functions, such as those related to network communication, file manipulation, and process injection
- I noticed various different scripts and payloads that should not be there executing.
- After the execution of the malware, it created several files that displayed on desktop.
- As I searched my device for other may be possible files that may have generated, I saw some of the files with suspicious names or extensions in system directories.
- As I noticed in IPA I can see that the exe file had built Connections to known and unknown malicious IP addresses or domains.
- As I checked my Regedit I found several New and modified registry keys related to autostart or persistence and I got several popup notifications related to the Malware file (e.g., Run, RunOnce keys).
- As I compared my Regshot File with my Regeditor directory I noticed the Creation of unusual registry keys or values.
- I experienced Changes in system behaviour such as unexpected system reboots or lagging

## **4.0**

### **CONCLUSION & RECOMMENDATIONS:**

This included a detailed analysis of malware behaviour and Windows Registry using different methods of static, dynamic and memory analysis. Here are the main results:

#### ❖ Static Analysis Findings

- Suspicious Strings: URLs that point to different unrecognisable website.
- File Headers and Metadata: Not signed, unusual attributes to evade detection.
- Imported Functions: Network communication, file manipulation, process injection.
- Embedded Resources: Encrypted payloads and scripts to hide the purpose.

#### ❖ Dynamic Analysis Findings:

- File System: Created files in system directories and modified critical application files.
- Network: Connected to external IP addresses. Connections were encrypted so we couldn't dig deeper into network traffic.
- Process and Service: New processes that looked like system processes and new services set to start automatically.
- Registry: Modified autostart registry keys to persist on the system. Also modified security settings to disable some protection.
- Behavioral: Ran unusual scripts and commands to spread or further compromise the system.

#### Registry Analysis:

- Autostart Entries: New entries found in autostart locations pointing to malicious executables.
- Security Settings Changes: Malware changed registry keys to turn off system defenses, firewall and security software.
- Persistence: Malware used multiple persistence mechanisms, scheduled tasks and WMI Event Consumers to stay active after reboots.

**Based on the findings above, here are the mitigations to reduce the risk of the malware and overall security:**

- **Block Malicious IPs and Domains:** Use threat intel feeds to block IPs and domains related to the malware.
- **Network Segmentation:** Segment critical systems and limit communication between segments to stop the malware spread.
- **Patch:** Keep your OS, apps and firmware up to date
- **Monitor Registry Changes:** Continuously monitor registry keys for unauthorized modifications, especially in autostart and security settings.
- **Quarantine and Eradicate Malware:** Immediately isolate infected systems to prevent further spread and perform thorough cleaning and recovery procedures.
- **Security Training:** Run regular training sessions on phishing, social engineering and safe computing.
- **Report Incidents:** Get users to report suspicious activity or potential security issues ASAP.

## **5.0**

### **LIST OF REFERENCES:**

<https://cuckoo.readthedocs.io/en/latest/installation/host/requirements>

[Setting up Cuckoo Sandbox Step by Step Guide\(Malware Analysis Tool\) | by Lahiru Oshara Hinguruduwa | Medium](#)

[regshot download | SourceForge.net](#)

[Wireshark · Go Deep](#)

[MalShare](#)

[PEiD - aldeid](#)

[IDA Free \(hex-rays.com\)](#)

[Windows 10 Professional 2024 Latest Download Preactivated - FileCR](#)

[Download Linux | Linux.org](#)

[Download Windows 7 ISO Files \(Direct Download Links\) \(itechtics.com\)](#)

<https://youtu.be/oPsxy9JF8FM?si=OhAitKWJyNfp2KUx>

[https://youtu.be/QIQS4gk\\_IFU?si=GGXdEsA9VzCACM50](https://youtu.be/QIQS4gk_IFU?si=GGXdEsA9VzCACM50)