Week 3: Digital Evidence Collection & Malware Analysis

What is FTK Imager?

FTK Imager is a powerful digital forensics tool developed by **Exterro (formerly AccessData)**. It is widely used by investigators to:

□ Key Functions:

- **Create forensic disk images** (bit-by-bit copies of hard drives, USBs, etc.)
- **Preview data without altering it** (read-only mode)
- **Recover deleted files**
- **Export files/folders**
- **Verify image integrity** using hash functions (MD5, SHA1)

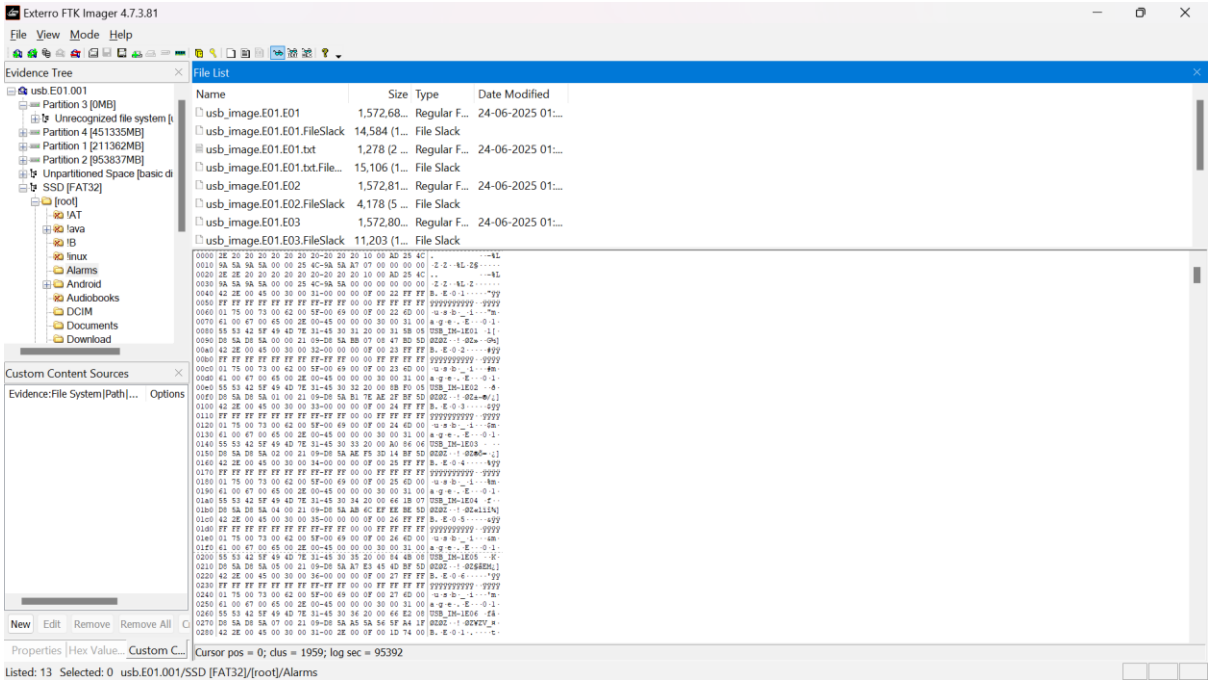
It supports multiple image formats like **E01**, **Raw (dd)**, and **AFF**, making it suitable for professional investigations and academic training.

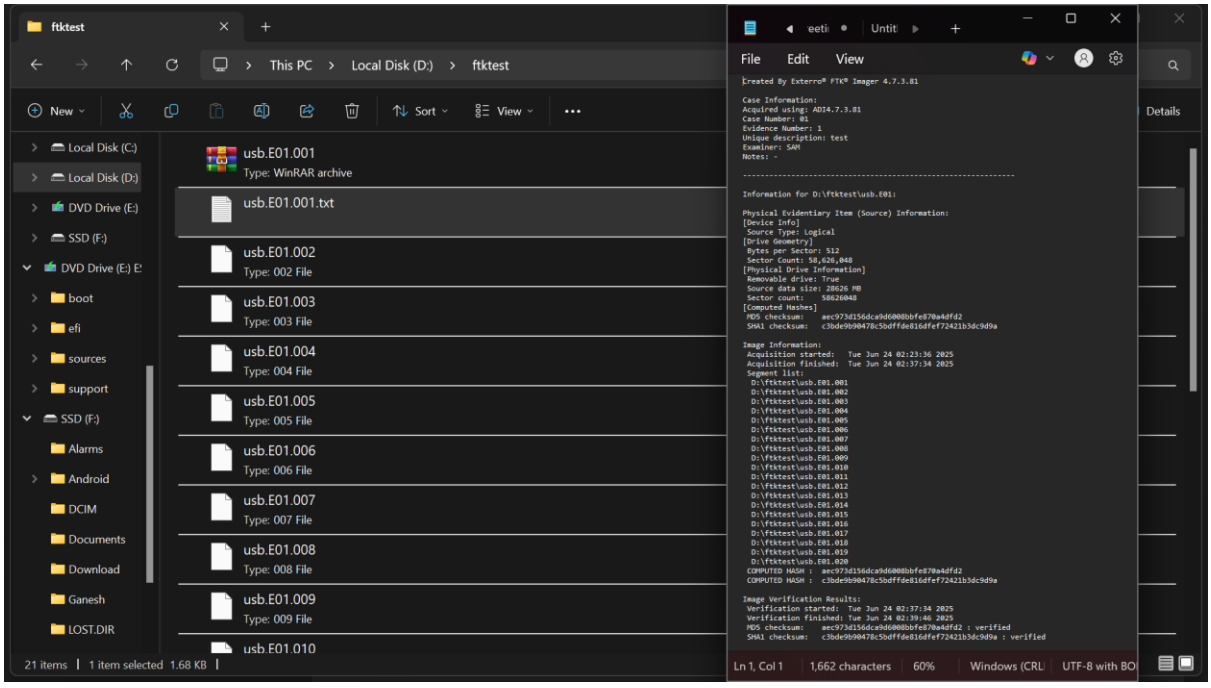
What I've Accomplished Using FTK Imager

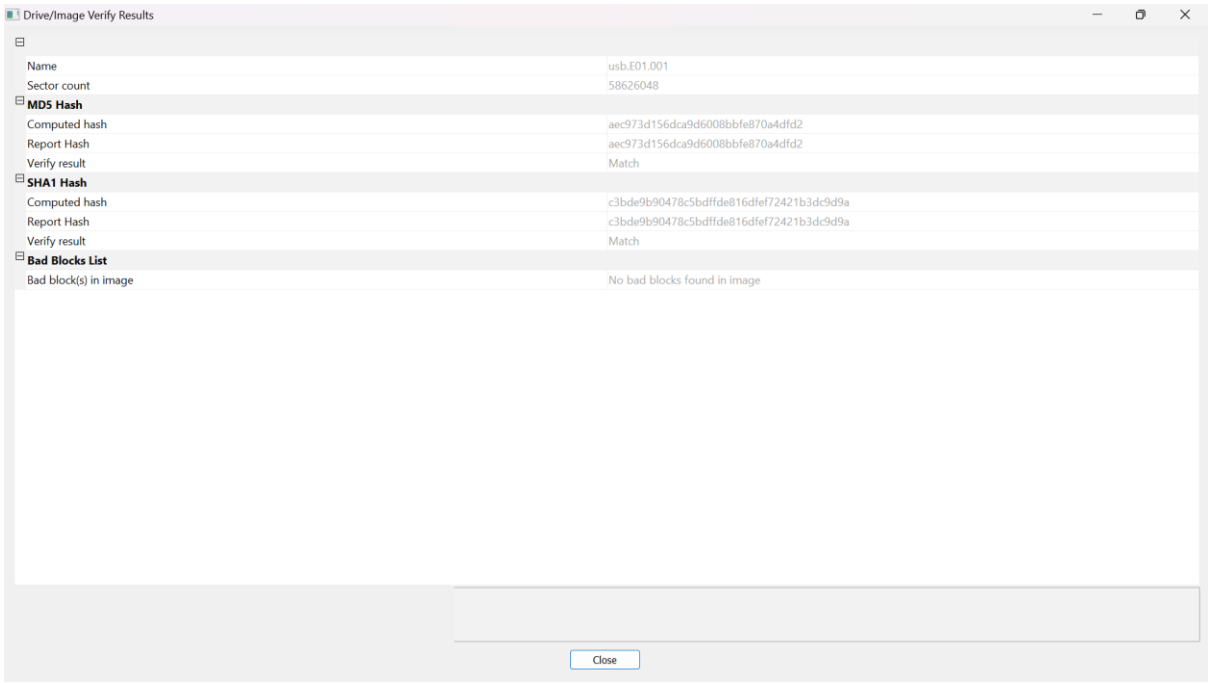
1. Disk Imaging (Evidence Acquisition)

I successfully:

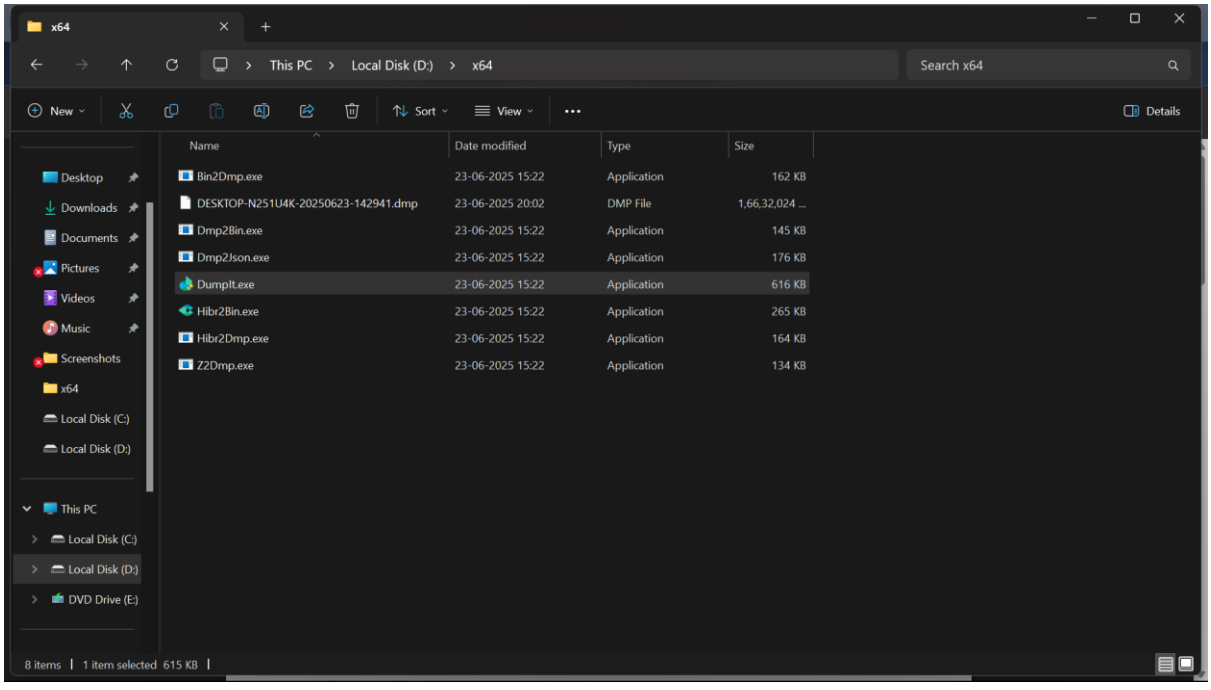
- Ran **FTK Imager as administrator**
- Selected a **Logical Drive (your USB)** for faster imaging
- Chose the **Raw (.dd) image format** for simplicity
- Saved the image to a separate drive (as required)
- Completed the imaging process and created:
    - A .dd image file
    - Logs with metadata and hash values (optional).

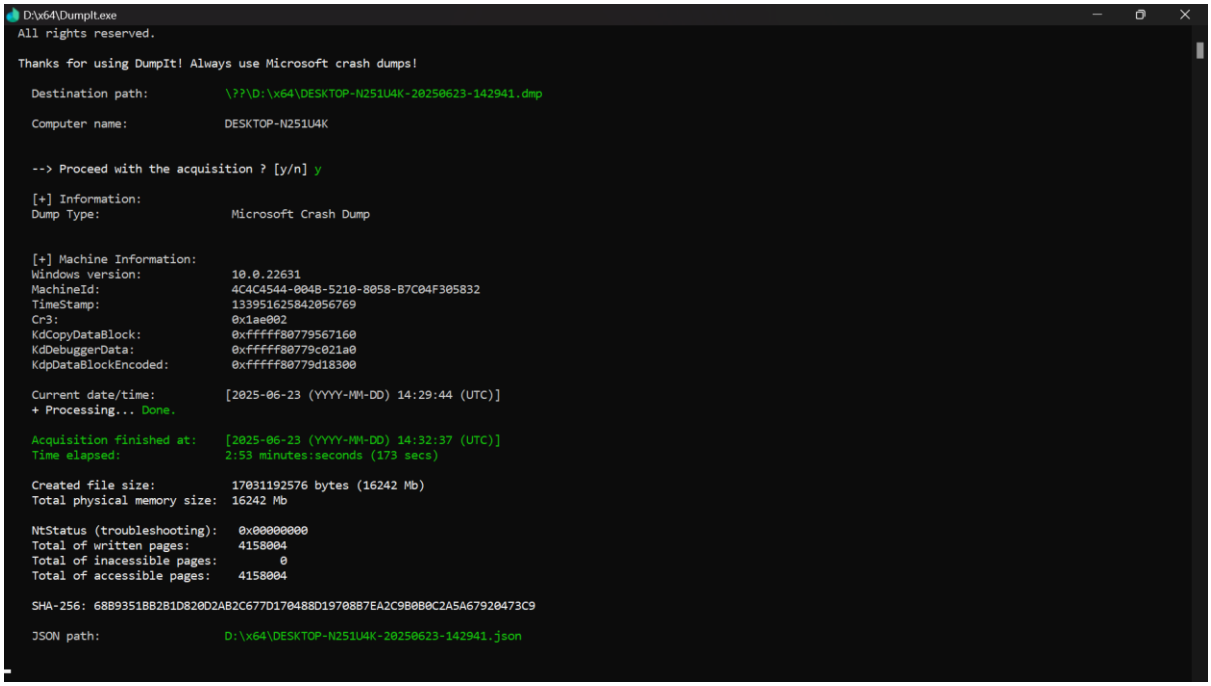

Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
usb.E01.001
Partition 3 [0MB]
Unrecognized file system [
Partition 4 [451335MB]
Partition 1 [211362MB]
Partition 2 [953837MB]
Unpartitioned Space [basic di
SSD [FAT32]
[root]
!AT
!ava
!B
linux
Alarms
Android
Audiobooks
DCIM
Documents
Download
Custom Content Sources
Evidence:File System|Path|...
Options
New Edit Remove Remove All
Properties Hex Value... Custom C...
File List
Name Size Type Date Modified
usb_image.E01.E01 1,572,68... Regular F... 24-06-2025 01:...
usb_image.E01.E01.FileSlack 14,584 (1... File Slack
usb_image.E01.E01.txt 1,278 (2 ... Regular F... 24-06-2025 01:...
usb_image.E01.E01.txt.File... 15,106 (1... File Slack
usb_image.E01.E02 1,572,81... Regular F... 24-06-2025 01:...
usb_image.E01.E02.FileSlack 4,178 (5 ... File Slack
usb_image.E01.E03 1,572,80... Regular F... 24-06-2025 01:...
usb_image.E01.E03.FileSlack 11,203 (1... File Slack
Cursor pos = 0; clus = 1959; log sec = 95392
Listed: 13 Selected: 0 usb.E01.001/SSD [FAT32]/[root]/Alarms


ftktest
This PC › Local Disk (D:) › ftktest
New Sort View
Local Disk (C:)
Local Disk (D:)
DVD Drive (E:)
SSD (F:)
DVD Drive (E:) E
boot
efi
sources
support
SSD (F:)
Alarms
Android
DCIM
Documents
Download
Ganesh
LOST.DIR
usb.E01.001
Type: WinRAR archive
usb.E01.001.txt
usb.E01.002
Type: 002 File
usb.E01.003
Type: 003 File
usb.E01.004
Type: 004 File
usb.E01.005
Type: 005 File
usb.E01.006
Type: 006 File
usb.E01.007
Type: 007 File
usb.E01.008
Type: 008 File
usb.E01.009
Type: 009 File
usb.E01.010
21 items 1 item selected 1.68 KB
File Edit View
Details
Ln 1, Col 1 1,662 characters 60% Windows (CRL UTF-8 with BO



Capture RAM with DumpIt.





What is Malware Analysis?

Malware analysis is the process of studying **malicious software** to understand its origin, functionality, and impact. The goal is to detect, contain, and neutralize threats posed by malware. Analysts use various techniques to reverse-engineer malware samples, monitor their behavior, and develop countermeasures. This field is crucial in **cybersecurity**, digital forensics, and incident response.

Malware Analysis Lab Setup (Windows 10 - VirtualBox)

To perform malware analysis safely and effectively, I set up a **fully isolated lab environment** using the following:

Virtualization Platform

- **Oracle VirtualBox** was used to create and manage virtual machines.
- I created a **Windows 10 VM** dedicated to malware testing.
- Network was configured to **Host-Only** or **Internal Network** to prevent malware from reaching the internet or host system.

Security Precautions

- **Snapshots** were taken before analysis to easily revert the VM.
- VM features like **drag-and-drop** and **shared folders** were disabled to prevent malware escape.
- Internet access was limited and monitored using **FakeNet-NG**.

FLARE VM – Malware Analysis Toolkit

I installed **FLARE VM (FireEye Labs Advanced Reverse Engineering VM)** — a specialized Windows-based platform for malware analysis. It includes:

- **Static Analysis Tools**: PEStudio, Detect It Easy, Resource Hacker
- **Dynamic Analysis Tools**: Process Hacker, Wireshark, Procmon, FakeNet-NG
- **Reverse Engineering Tools**: IDA Free, x64dbg, .NET Reflector
- **Automation & Forensics**: Volatility, Autoruns, Strings

Installation was done using a PowerShell script (install.ps1) from the FLARE VM GitHub repo. The setup required around **60 GB of disk space** and several hours of tool installation.

Static malware analysis steps

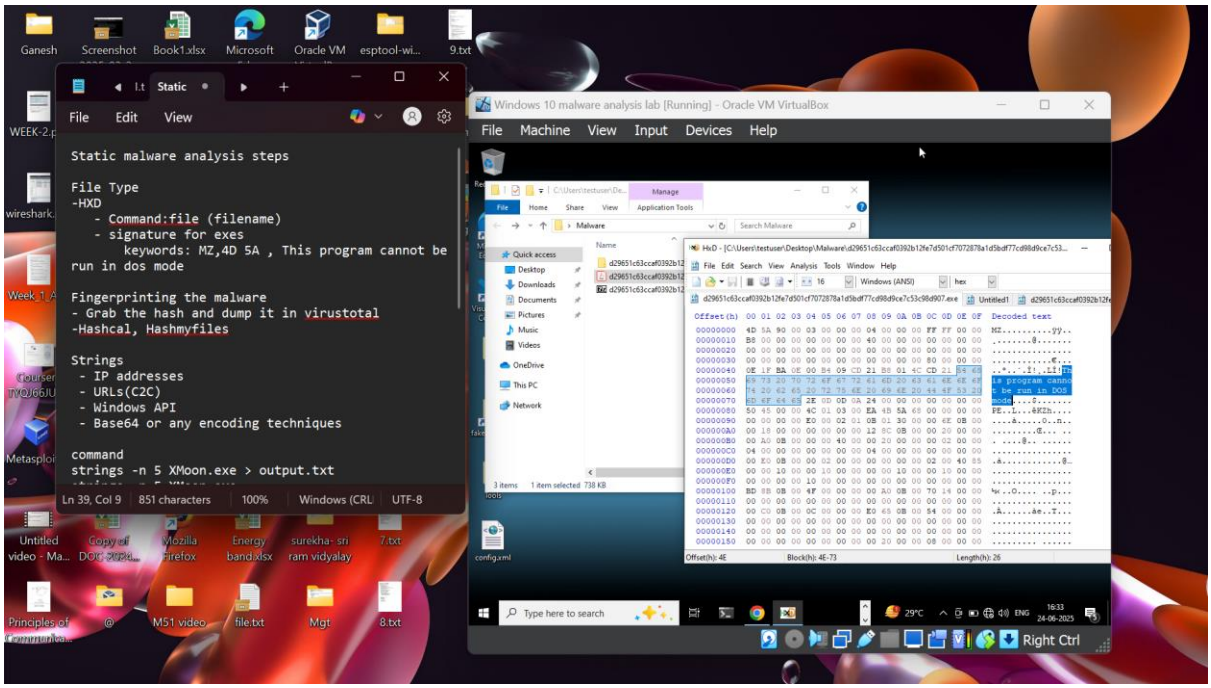
File Type

-HXD

- Command:file (filename)

- signature for exes

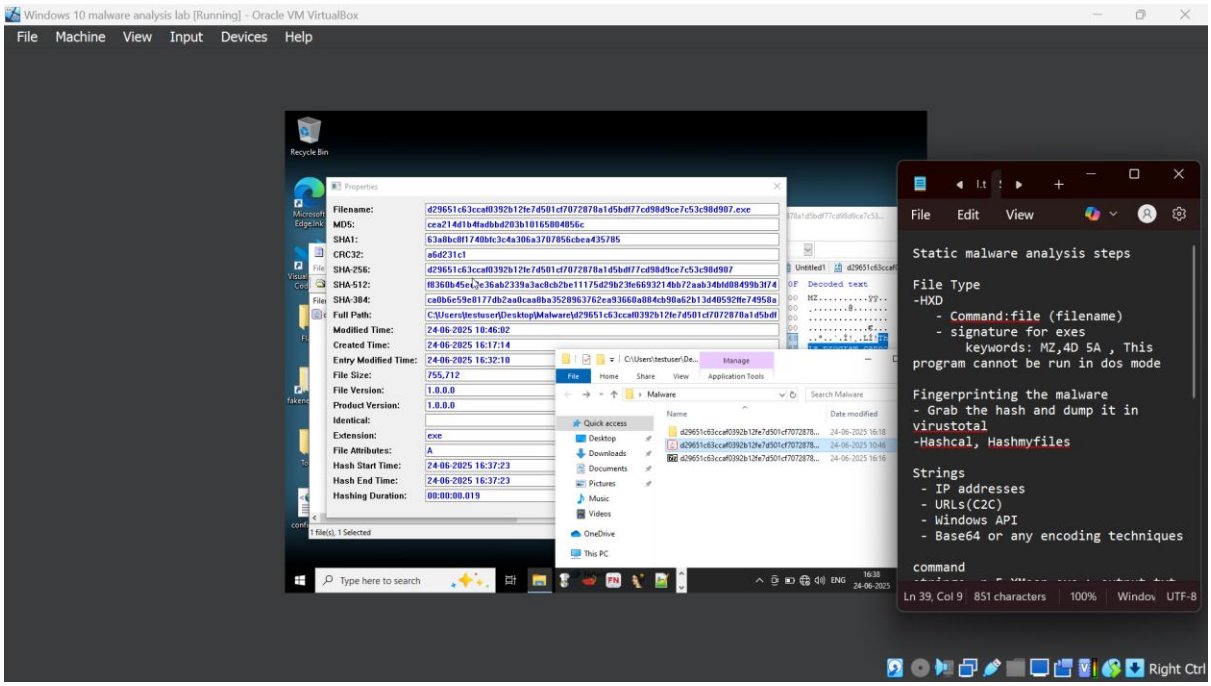
keywords: MZ,4D 5A , This program cannot be run in dos mode

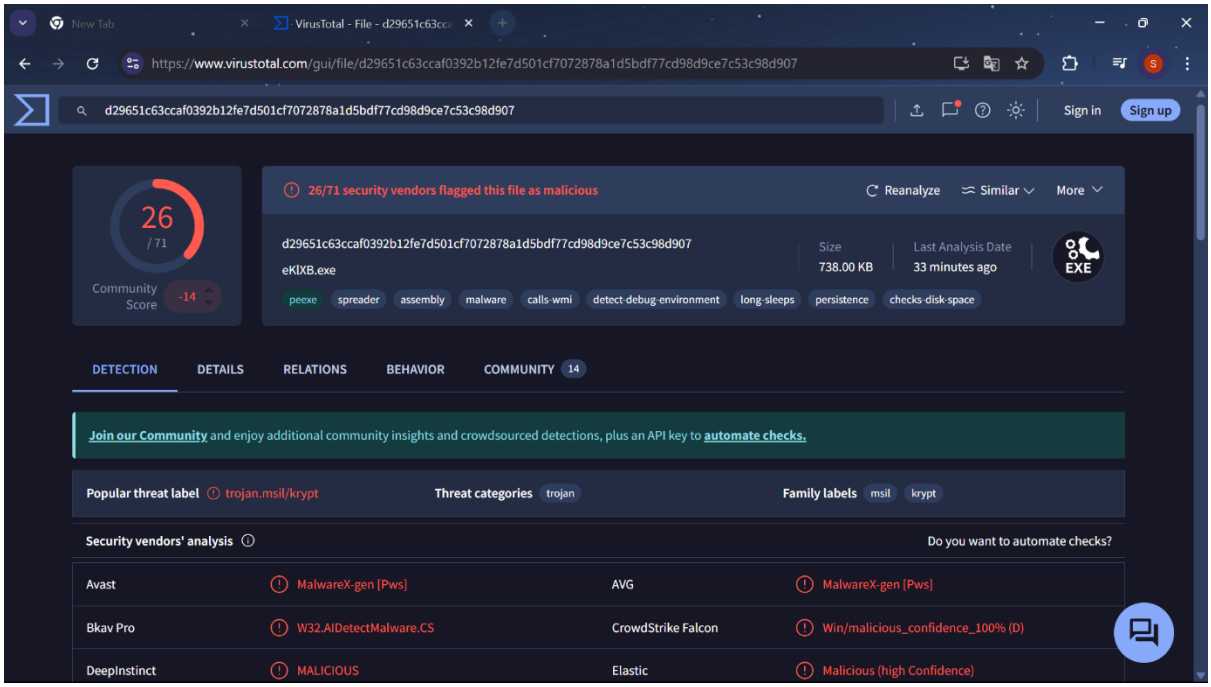


Fingerprinting the malware

- Grab the hash and dump it in virustotal

-Hashcal, Hashmyfiles





Strings

- IP addresses

- URLs(C2C)

- Windows API

- Base64 or any encoding techniques

command

strings -n 5 XMoon.exe > output.txt

strings -n 5 XMoon.exe

Decrypting Encoded strings

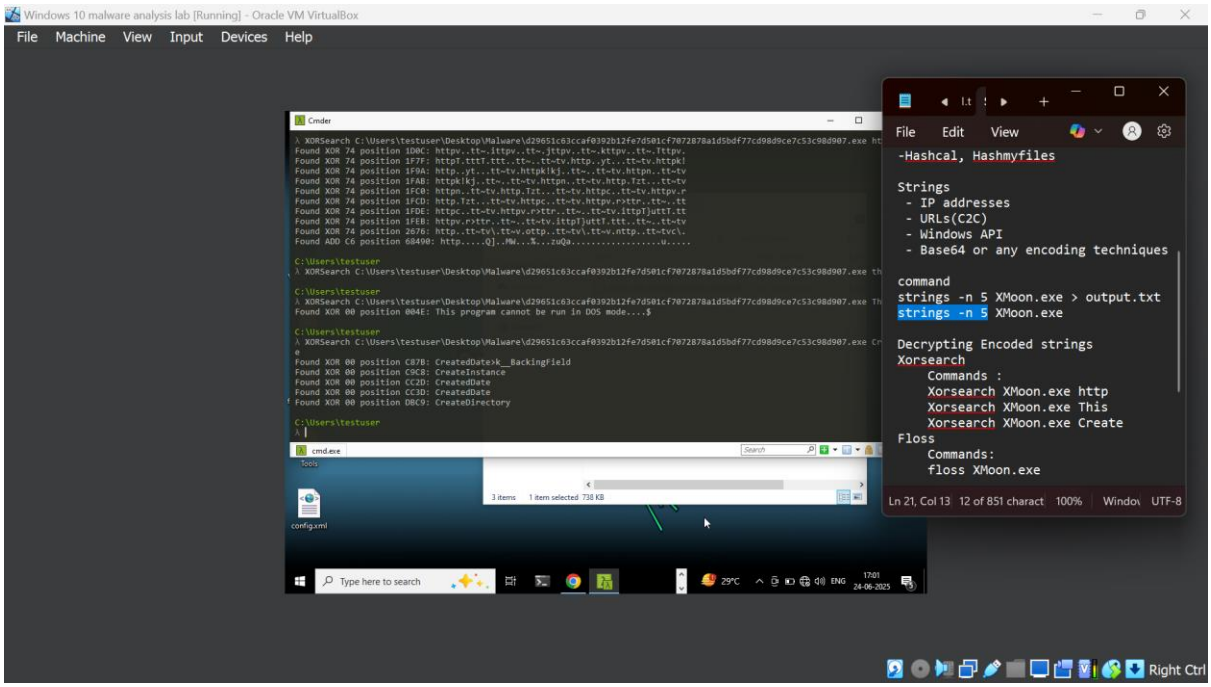
Xorsearch

Commands :

Xorsearch XMoon.exe http

Xorsearch XMoon.exe This

Xorsearch XMoon.exe Create



Floss

Commands:

floss XMoon.exe

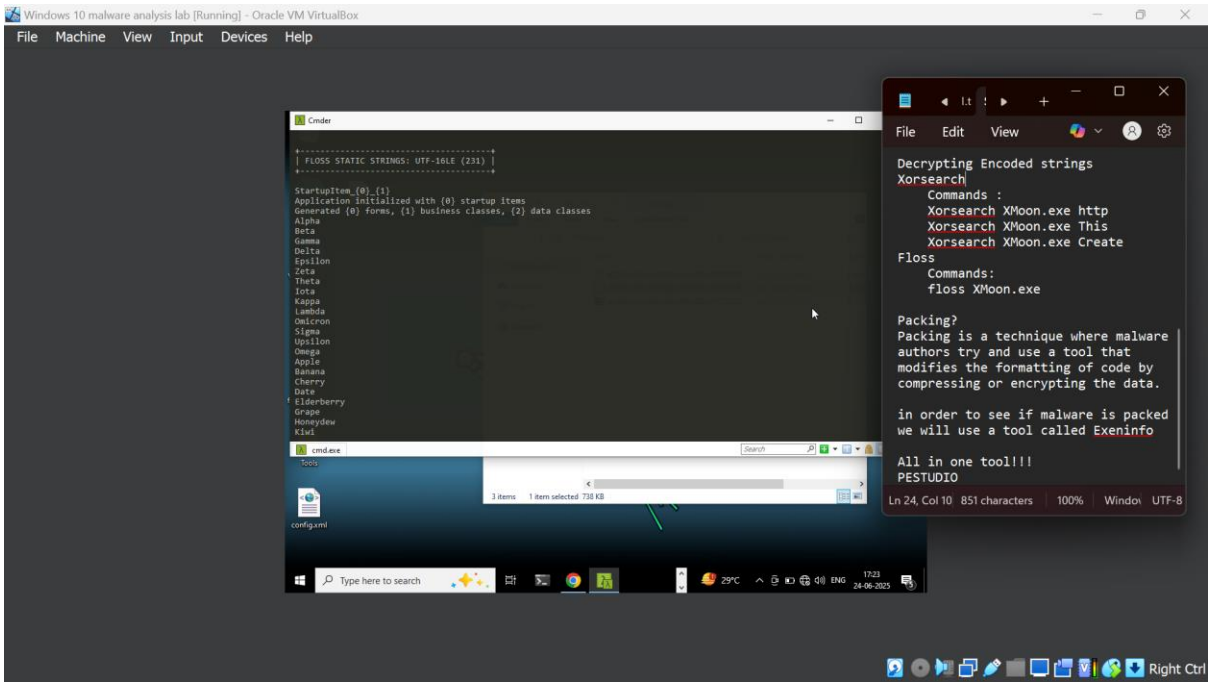
Packing?

Packing is a technique where malware authors try and use a tool that modifies the formatting of code by compressing or encrypting the data.

in order to see if malware is packed we will use a tool called Exeninfo

All in one tool!!!

PESTUDIO



Dynamic Malware Analysis:

4 Things to look for:

-Process Hacker

-Procmon

Network Activity : Look for C2 servers because malware steals data and sends it to the malware author

-Wireshark(Fliter or smtp, http, DNS)

Registry Activities(Persistance)

-Regshot:(Keys added, values added, values modified, files added)

-procmon

keys to look for when it comes to startup

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce

File Activities (Presistence)

-regshot

-Procmon

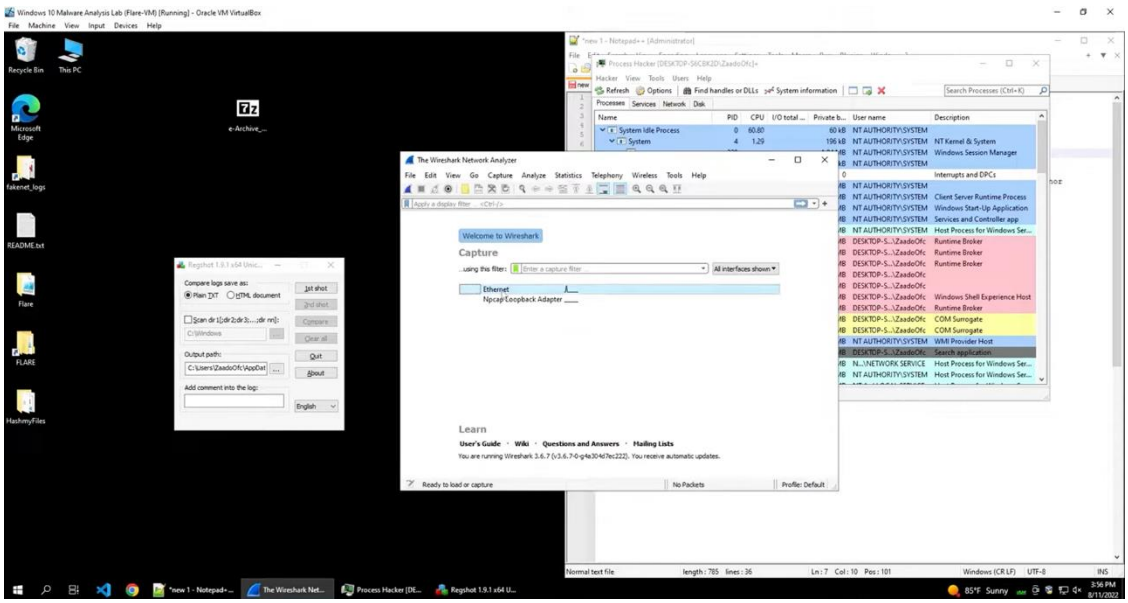
-"C:\Users\Username\AppData\Roaming\"

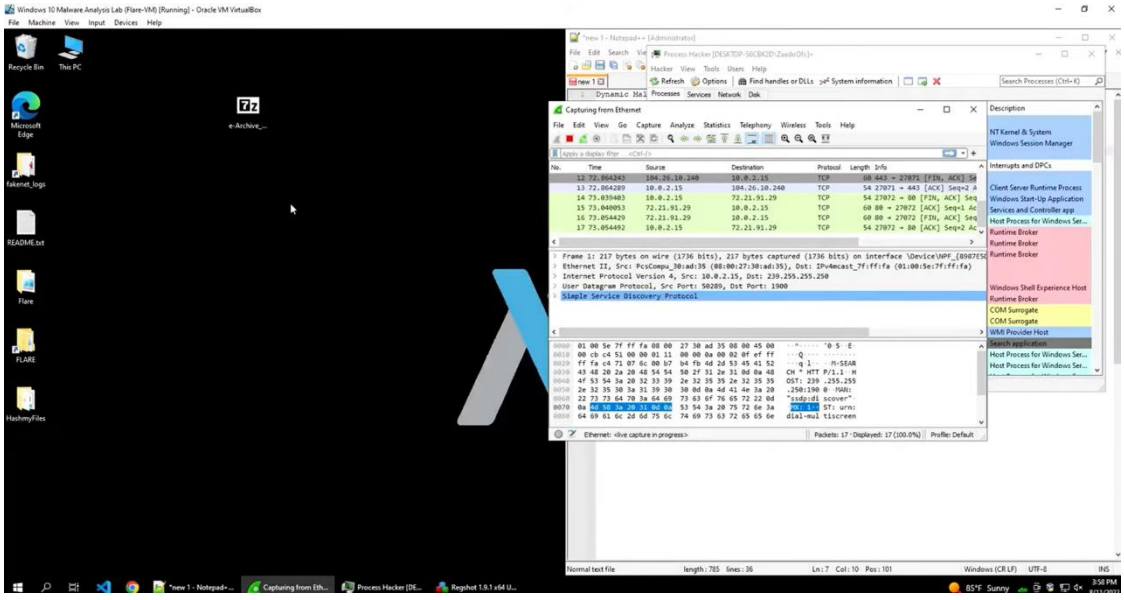
Windows+R

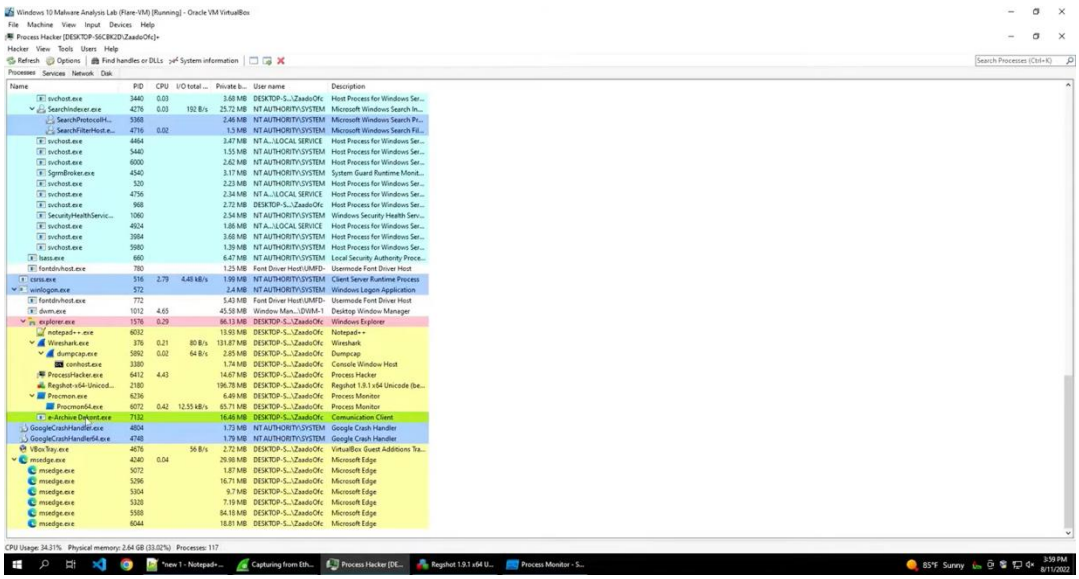
%temp%

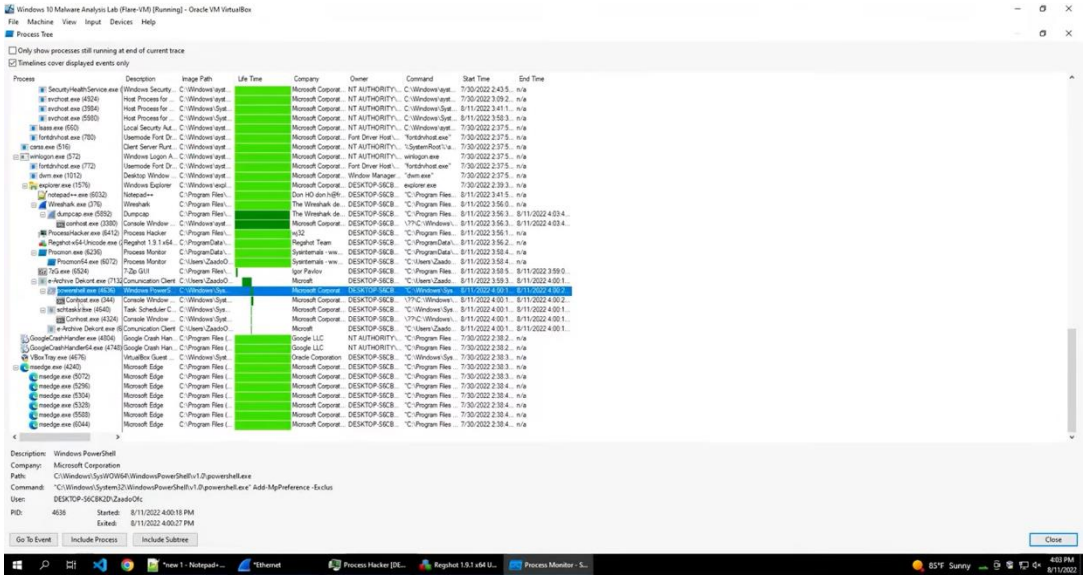
shell:startup

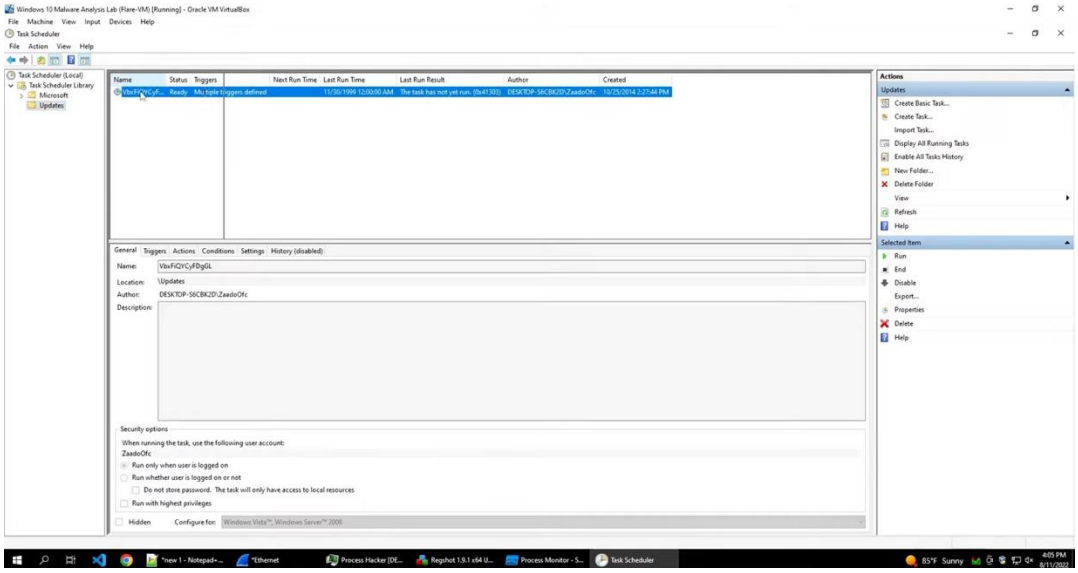
shell:common startup

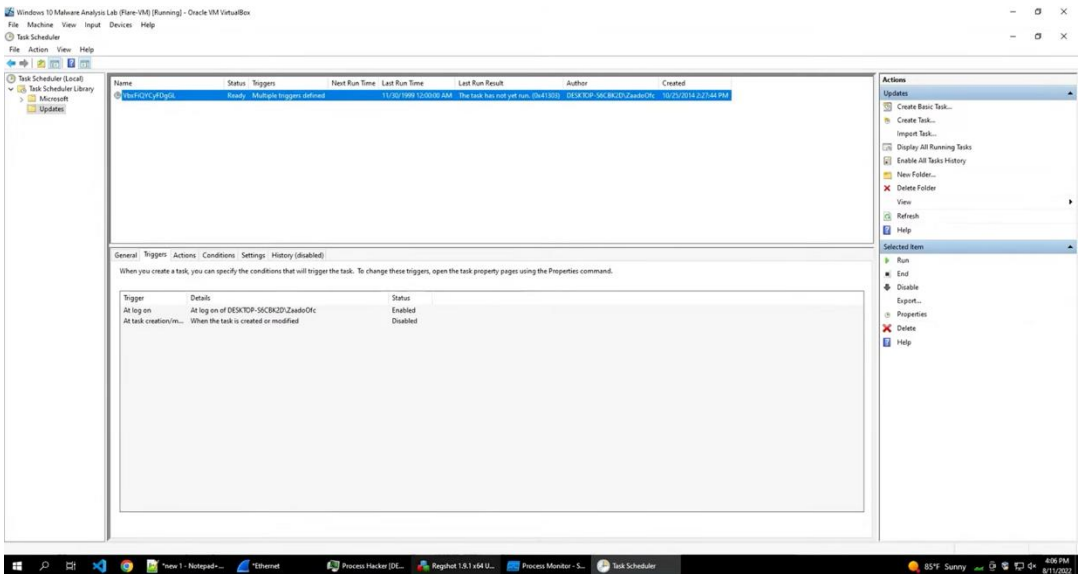


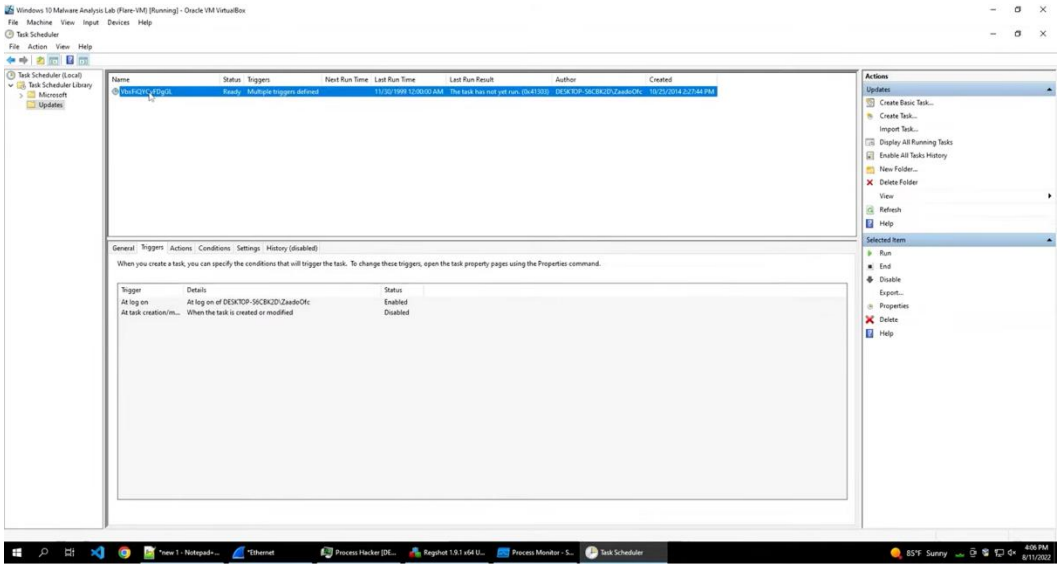


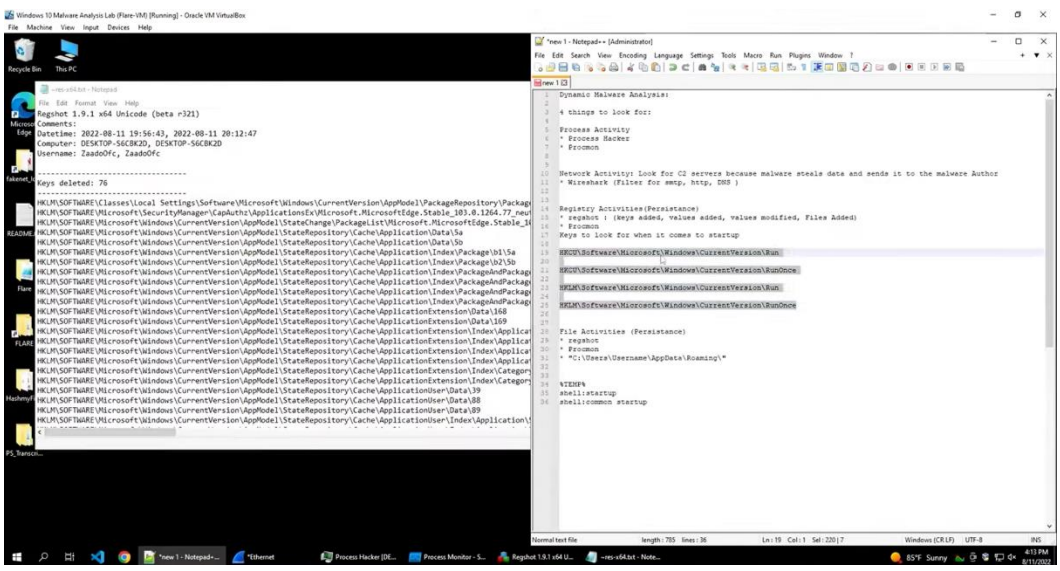


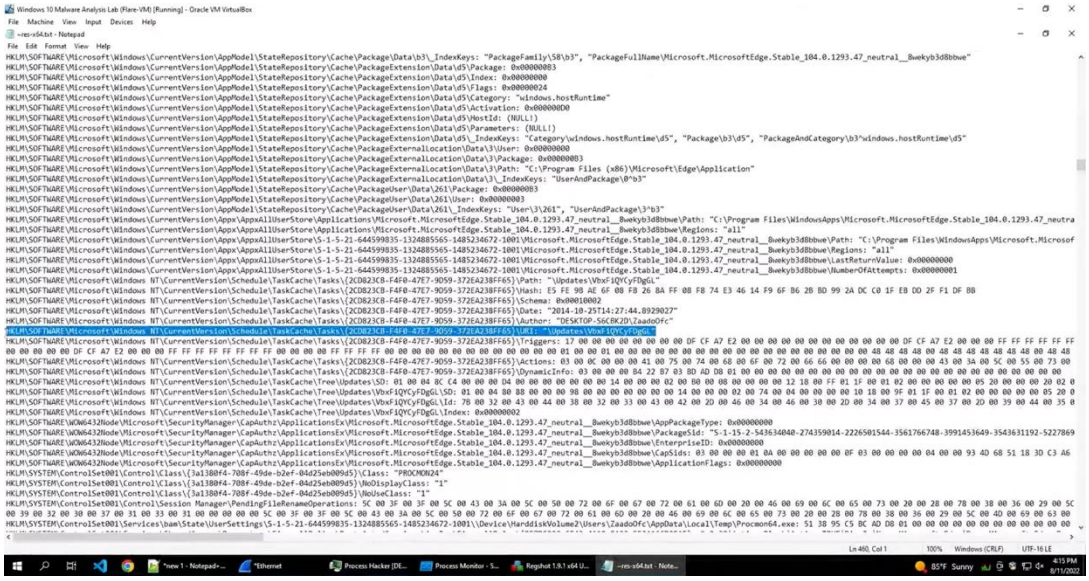


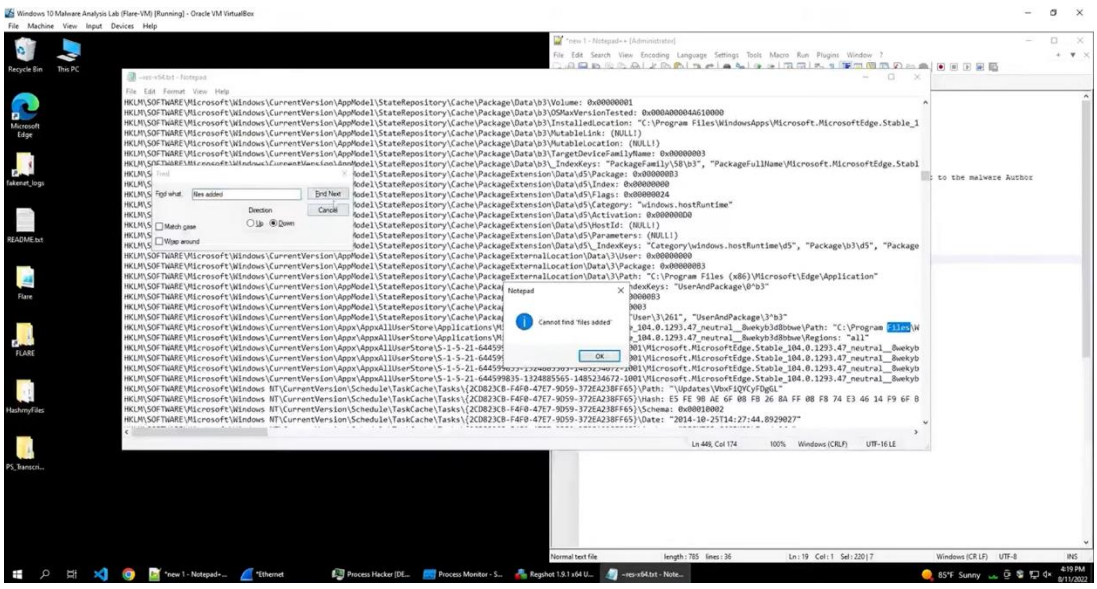


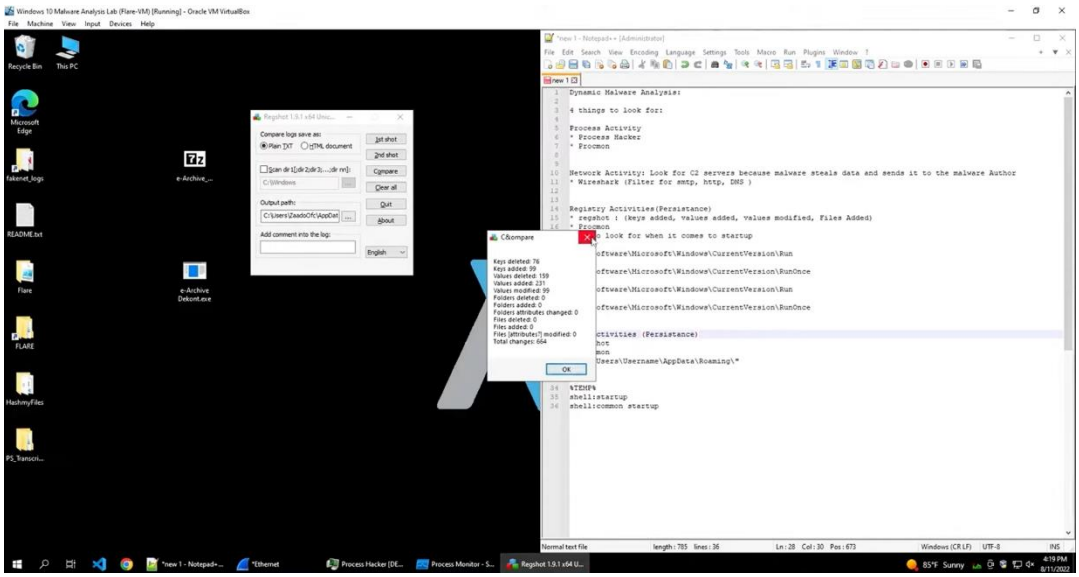

Windows 10 Malware Analysis Lab (Flare-VM) [Running] - Oracle VM VirtualBox
Task Scheduler
Task Scheduler (Local)
Task Scheduler Library
Microsoft
Updates
Name
Status
Triggers
Next Run Time
Last Run Time
Last Run Result
Author
Created
VbsFiQYCyFDgGL
Ready
Multiple triggers defined
11/30/1999 12:00:00 AM
The task has not yet run. (0x41303)
DESKTOP-S6CBK2D\ZaadoOfc
10/25/2014 2:27:44 PM
General
Triggers
Actions
Conditions
Settings
History (disabled)
When you create a task, you can specify the conditions that will trigger the task. To change these triggers, open the task property pages using the Properties command.
Trigger
Details
Status
At log on
At log on of DESKTOP-S6CBK2D\ZaadoOfc
Enabled
At task creation/m...
When the task is created or modified
Disabled
Actions
Create Basic Task...
Create Task...
Import Task...
Display All Running Tasks
Enable All Tasks History
New Folder...
Delete Folder
View
Refresh
Help
Selected Item
Run
End
Disable
Export...
Properties
Delete
Help
85°F Sunny
4:06 PM
8/11/2022


Windows 10 Malware Analysis Lab (Flare-VM) [Running] - Oracle VM VirtualBox
Task Scheduler
Task Scheduler (Local)
Task Scheduler Library
Microsoft
Updates
Name
Status
Triggers
Next Run Time
Last Run Time
Last Run Result
Author
Created
VbsFiQYCyFDgGL
Ready
Multiple triggers defined
11/30/1999 12:00:00 AM
The task has not yet run. (0x41303)
DESKTOP-S6CBK2D\ZaadoOfc
10/25/2014 2:27:44 PM
General
Triggers
Actions
Conditions
Settings
History (disabled)
When you create a task, you can specify the conditions that will trigger the task. To change these triggers, open the task property pages using the Properties command.
Trigger
Details
Status
At log on
At log on of DESKTOP-S6CBK2D\ZaadoOfc
Enabled
At task creation/m...
When the task is created or modified
Disabled
Actions
Create Basic Task...
Create Task...
Import Task...
Display All Running Tasks
Enable All Tasks History
New Folder...
Delete Folder
View
Refresh
Help
Selected Item
Run
End
Disable
Export...
Properties
Delete
Help
85°F Sunny
4:06 PM
8/11/2022


Windows 10 Malware Analysis Lab (Flare-VM) [Running] - Oracle VM VirtualBox
Recycle Bin
This PC
--res-x64.txt - Notepad
Regshot 1.9.1 x64 Unicode (beta r321)
Comments:
Datetime: 2022-08-11 19:56:43, 2022-08-11 20:12:47
Computer: DESKTOP-S6CBK2D, DESKTOP-S6CBK2D
Username: ZaadoOfc, ZaadoOfc
Keys deleted: 76
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packag
HKLM\SOFTWARE\Microsoft\SecurityManager\CapAuthz\ApplicationsEx\Microsoft.MicrosoftEdge.Stable_103.0.1264.77_neu
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateChange\PackageList\Microsoft.MicrosoftEdge.Stable_1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Application\Data\5a
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Application\Data\5b
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Application\Index\Package\b1\5a
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Application\Index\Package\b2\5b
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Application\Index\PackageAndPackag
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Application\Index\PackageAndPackag
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Application\Index\PackageAndPackag
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Application\Index\PackageAndPackag
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationExtension\Data\168
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationExtension\Data\169
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationExtension\Index\Applica
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationExtension\Index\Applica
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationExtension\Index\Applica
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationExtension\Index\Categor
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationExtension\Index\Categor
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationUser\Data\139
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationUser\Data\88
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationUser\Data\89
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationUser\Index\Application\
"new 1 - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
new 1
Dynamic Malware Analysis:
4 things to look for:
Process Activity
* Process Hacker
* Procmon
Network Activity: Look for C2 servers because malware steals data and sends it to the malware Author
* Wireshark (Filter for smtp, http, DNS)
Registry Activities(Persistance)
* regshot 1 (keys added, values added, values modified, Files Added)
* Procmon
Keys to look for when it comes to startup
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
File Activities (Persistance)
* regshot
* Procmon
* "C:\Users\Username\AppData\Roaming\"
%TEMP%
shell:startup
shell:common startup
Normal text file
length : 785 lines : 36
Ln : 19 Col : 1 Sel : 220 | 7
Windows (CR LF)
UTF-8
INS
85°F Sunny
4:13 PM
8/11/2022


Windows 10 Malware Analysis Lab (Flare-VM) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
~res-x64.txt - Notepad
File Edit Format View Help
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Package\Data\b3_IndexKeys: "PackageFamily\$8\b3", "PackageFullName\Microsoft.MicrosoftEdge.Stable_104.0.1293.47_neutral__8wekyb3d8bbwe"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\PackageExtension\Data\d5\Package: 0x00000003
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\PackageExtension\Data\d5\Index: 0x00000000
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\PackageExtension\Data\d5\Flags: 0x00000024
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\PackageExtension\Data\d5\Category: "windows.hostRuntime"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\PackageExtension\Data\d5\Activation: 0x000000D0
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\PackageExtension\Data\d5\HostId: (NULL!)
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\PackageExtension\Data\d5\Parameters: (NULL!)
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\PackageExtension\Data\d5_IndexKeys: "Category\windows.hostRuntime\d5", "Package\b3\d5", "PackageAndCategory\b3"windows.hostRuntime\d5"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\PackageExternalLocation\Data\3\User: 0x00000000
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\PackageExternalLocation\Data\3\Package: 0x00000003
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\PackageExternalLocation\Data\3\Path: "C:\Program Files (x86)\Microsoft\Edge\Application"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\PackageExternalLocation\Data\3_IndexKeys: "UserAndPackage\0"b3"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\PackageUser\Data\261\Package: 0x00000003
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\PackageUser\Data\261\User: 0x00000003
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\PackageUser\Data\261_IndexKeys: "User\3\261", "UserAndPackage\3"b3"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Apps\AppxAllUserStore\Applications\Microsoft.MicrosoftEdge.Stable_104.0.1293.47_neutral__8wekyb3d8bbwe\Path: "C:\Program Files\WindowsApps\Microsoft.MicrosoftEdge.Stable_104.0.1293.47_neutra
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Apps\AppxAllUserStore\Applications\Microsoft.MicrosoftEdge.Stable_104.0.1293.47_neutral__8wekyb3d8bbwe\Regions: "all"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Apps\AppxAllUserStore\S-1-5-21-644599835-1324885565-1485234672-1001\Microsoft.MicrosoftEdge.Stable_104.0.1293.47_neutral__8wekyb3d8bbwe\Path: "C:\Program Files\WindowsApps\Microsof
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Apps\AppxAllUserStore\S-1-5-21-644599835-1324885565-1485234672-1001\Microsoft.MicrosoftEdge.Stable_104.0.1293.47_neutral__8wekyb3d8bbwe\Regions: "all"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Apps\AppxAllUserStore\S-1-5-21-644599835-1324885565-1485234672-1001\Microsoft.MicrosoftEdge.Stable_104.0.1293.47_neutral__8wekyb3d8bbwe\LastReturnValue: 0x00000000
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Apps\AppxAllUserStore\S-1-5-21-644599835-1324885565-1485234672-1001\Microsoft.MicrosoftEdge.Stable_104.0.1293.47_neutral__8wekyb3d8bbwe\NumberOfAttempts: 0x00000001
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{2CD823C8-F4F0-47E7-9D59-372EA238FF65}\Path: "\Updates\VbxFiQYCyFDgGL"
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{2CD823C8-F4F0-47E7-9D59-372EA238FF65}\Hash: E5 FE 98 AE 6F 08 FB 26 8A FF 08 F8 74 E3 46 14 F9 6F B6 2B BD 99 2A DC C0 1F EB DD 2F F1 DF BB
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{2CD823C8-F4F0-47E7-9D59-372EA238FF65}\Schema: 0x00010002
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{2CD823C8-F4F0-47E7-9D59-372EA238FF65}\Date: "2014-10-25T14:27:44.8929027"
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{2CD823C8-F4F0-47E7-9D59-372EA238FF65}\Author: "DESKTOP-S6CBK2D\ZaadoOfc"
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{2CD823C8-F4F0-47E7-9D59-372EA238FF65}\UKI: "\Updates\VbxFiQYCyFDgGL"
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{2CD823C8-F4F0-47E7-9D59-372EA238FF65}\Triggers: 17 00 00 00 00 00 00 00 00 00 00 00 00 00 DF CF A7 E2 00 00 00 00 00 00 00 00 00 00 DF CF A7 E2 00 00 00 FF FF FF FF FF FF
00 00 00 00 00 DF CF A7 E2 00 00 00 FF FF FF FF FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 48 48 48 00 48 48 48 48 48 48 48 00 48 48
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{2CD823C8-F4F0-47E7-9D59-372EA238FF65}\Actions: 03 00 0C 00 00 00 41 00 75 00 74 00 68 00 6F 00 72 00 66 66 00 00 00 00 68 00 00 00 43 00 3A 00 5C 00 55 00 73 00
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{2CD823C8-F4F0-47E7-9D59-372EA238FF65}\DynamicInfo: 03 00 00 00 84 22 B7 03 BD AD D8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Updates\SD: 01 00 04 8C C4 00 00 00 D4 00 00 00 00 00 00 00 14 00 00 00 02 00 70 00 04 00 00 00 00 00 14 00 00 00 02 00 74 00 04 00 00 00 00 00 12 18 00 FF 01 1F 00 01 02 00 00 00 00 00 05 20 00 00 00 20 02 0
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Updates\SD: 01 00 04 80 B8 00 00 00 98 00 00 00 00 00 00 00 14 00 00 00 02 00 74 00 04 00 00 00 00 00 10 18 00 9F 01 1F 00 01 02 00 00 00 00 00 05 20 0
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Updates\VbxFiQYCyFDgGL\Id: 7B 00 32 00 43 00 44 00 38 00 32 00 33 00 43 00 42 00 2D 00 46 00 34 00 46 00 38 00 2D 00 34 00 37 00 45 00 37 00 2D 00 39 00 44 00 35 0
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Updates\VbxFiQYCyFDgGL\Index: 0x00000002
HKLM\SOFTWARE\WOW6432Node\Microsoft\SecurityManager\CapAuthz\ApplicationsEx\Microsoft.MicrosoftEdge_Stable_104.0.1293.47_neutral__8wekyb3d8bbwe\AppPackageType: 0x00000000
HKLM\SOFTWARE\WOW6432Node\Microsoft\SecurityManager\CapAuthz\ApplicationsEx\Microsoft.MicrosoftEdge_Stable_104.0.1293.47_neutral__8wekyb3d8bbwe\PackageSid: "S-1-15-2-543634040-274359014-2226501544-3561766748-3991453649-3543631192-5227869
HKLM\SOFTWARE\WOW6432Node\Microsoft\SecurityManager\CapAuthz\ApplicationsEx\Microsoft.MicrosoftEdge_Stable_104.0.1293.47_neutral__8wekyb3d8bbwe\EnterpriseID: 0x00000000
HKLM\SOFTWARE\WOW6432Node\Microsoft\SecurityManager\CapAuthz\ApplicationsEx\Microsoft.MicrosoftEdge_Stable_104.0.1293.47_neutral__8wekyb3d8bbwe\CapSids: 03 00 00 00 01 8A 00 00 00 00 00 0F 03 00 00 00 00 04 00 00 93 4D 68 51 18 3D C3 A6
HKLM\SOFTWARE\WOW6432Node\Microsoft\SecurityManager\CapAuthz\ApplicationsEx\Microsoft.MicrosoftEdge_Stable_104.0.1293.47_neutral__8wekyb3d8bbwe\ApplicationFlags: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\Class\{3a1380f4-708f-49de-b2ef-04d25eb009d5}\Class: "PROCMON24"
HKLM\SYSTEM\ControlSet001\Control\Class\{3a1380f4-708f-49de-b2ef-04d25eb009d5}\NoDisplayClass: "1"
HKLM\SYSTEM\ControlSet001\Control\Class\{3a1380f4-708f-49de-b2ef-04d25eb009d5}\NoUseClass: "1"
HKLM\SYSTEM\ControlSet001\Control\Session Manager\PendingFileRenameOperations: 5C 00 3F 00 3F 00 5C 00 43 00 3A 00 5C 00 50 00 72 00 6F 00 67 00 72 00 61 00 6D 00 20 00 46 00 69 00 6C 00 65 00 73 00 20 00 28 00 78 00 38 00 36 00 29 00 5C
00 39 00 32 00 30 00 37 00 31 00 33 00 31 00 00 00 00 00 5C 00 3F 00 3F 00 5C 00 43 00 3A 00 5C 00 50 00 72 00 6F 00 67 00 72 00 61 00 6D 00 20 00 46 00 69 00 6C 00 65 00 73 00 20 00 28 00 78 00 38 00 36 00 29 00 5C 00 4D 00 69 00 63 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-644599835-1324885565-1485234672-1001\\Device\HarddiskVolume2\Users\ZaadoOfc\AppData\Local\Temp\Procmon64.exe: 51 3B 95 C5 BC AD D8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Ln 460, Col 1
100%
Windows (CRLF)
UTF-16 LE
Recycle Bin
This PC
Microsoft Edge
fakenet_logs
README.txt
Flare
FLARE
HashmyFiles
PS_Transcri...
*new 1 - Notepad++...
*Ethernet
Process Hacker [DE...
Process Monitor - S...
Regshot 1.9.1 x64 U...
~res-x64.txt - Note...
85°F Sunny
4:15 PM
8/11/2022


Windows 10 Malware Analysis Lab (Flare-VM) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
~res-x64.txt - Notepad
Find what: files added
Direction
Up
Down
Match case
Wrap around
Find Next
Cancel
Notepad
Cannot find 'files added'
OK
Ln 449, Col 174
100%
Windows (CRLF)
UTF-16 LE
*new 1 - Notepad++ [Administrator]
Normal text file
length : 785 lines : 36
Ln : 19 Col : 1 Sel : 220 | 7
Windows (CR LF)
UTF-8
INS
4:19 PM
8/11/2022


Windows 10 Malware Analysis Lab (Flare-VM) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Regshot 1.9.1 x64 Unico...
Compare logs save as:
Plain TXT
HTML document
1st shot
2nd shot
Compare
Clear all
Quit
About
Output path:
C:\Users\ZaadoOfc\AppDat
Add comment into the log:
English
e-Archive_...
e-Archive Dekont.exe
CAcompare
Keys deleted: 76
Keys added: 99
Values deleted: 159
Values added: 231
Values modified: 99
Folders deleted: 0
Folders added: 0
Folders attributes changed: 0
Files deleted: 0
Files added: 0
Files [attributes?] modified: 0
Total changes: 664
OK
*new 1 - Notepad++ [Administrator]
1 Dynamic Malware Analysis:
3 4 things to look for:
5 Process Activity
6 * Process Hacker
7 * Procmon
10 Network Activity: Look for C2 servers because malware steals data and sends it to the malware Author
11 * Wireshark (Filter for smtp, http, DNS)
14 Registry Activities(Persistance)
15 * regshot : (keys added, values added, values modified, Files Added)
16 * Procmon
17 -> look for when it comes to startup
34 %TEMP%
35 shell:startup
36 shell:common startup
Normal text file
length : 785 lines : 36
Ln : 28 Col : 30 Pos : 673
Windows (CR LF)
UTF-8
INS
4:19 PM
8/11/2022