MALWARE ANALYSIS

Team
Abdallah Hamdan
Inaam kabbara
Shiron dev Newton

Table of Contents

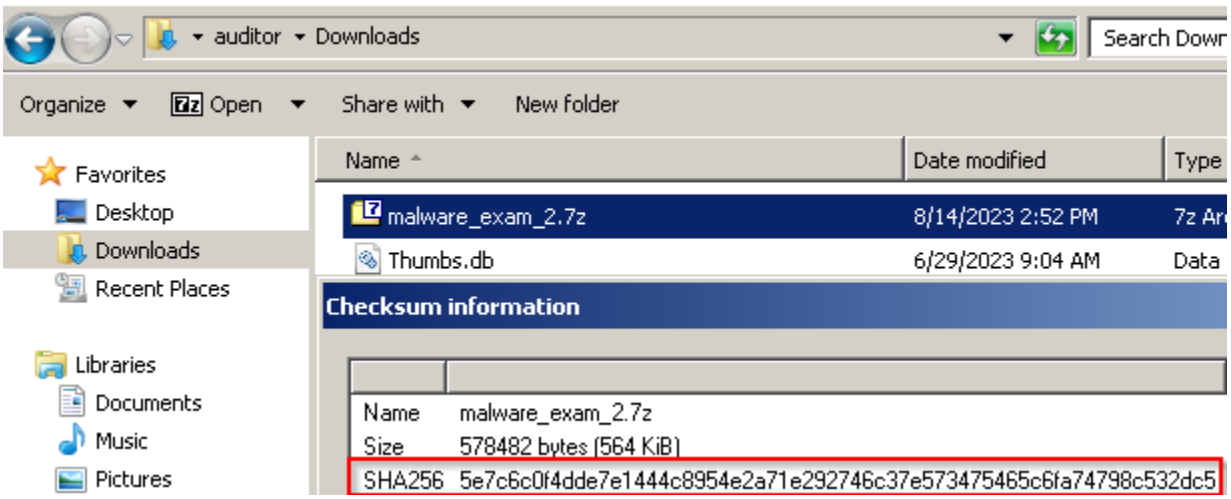
1. Static analysis: malware_exam_2.7z

The analysis primarily start with first file and file type is 7zip. Further analysis done using statically since to identify further information before targeting the dynamic analysis.

Following documentations are the steps and information provided by the analysis team in order to identify the functionality of the malware.

File hash:

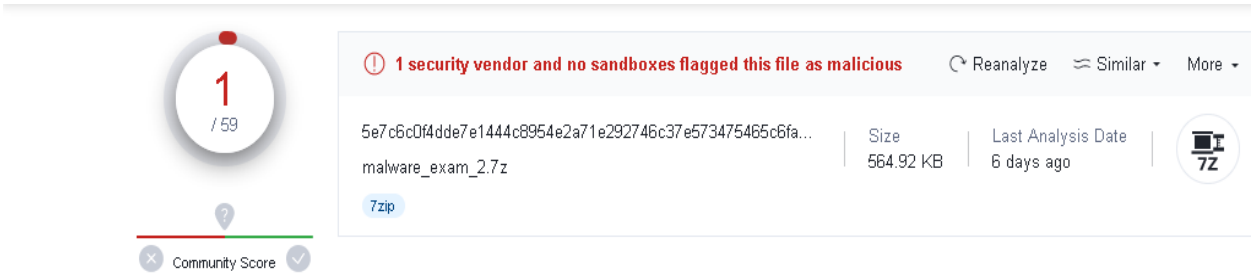
SHA-256 - 5e7c6c0f4dde7e1444c8954e2a71e292746c37e573475465c6fa74798c532dc5



The first document contains the sha 256 hash and when googled no further information was provided or documented so investing time on to this, the analysis went to next stage of gathering more information regarding the malware.

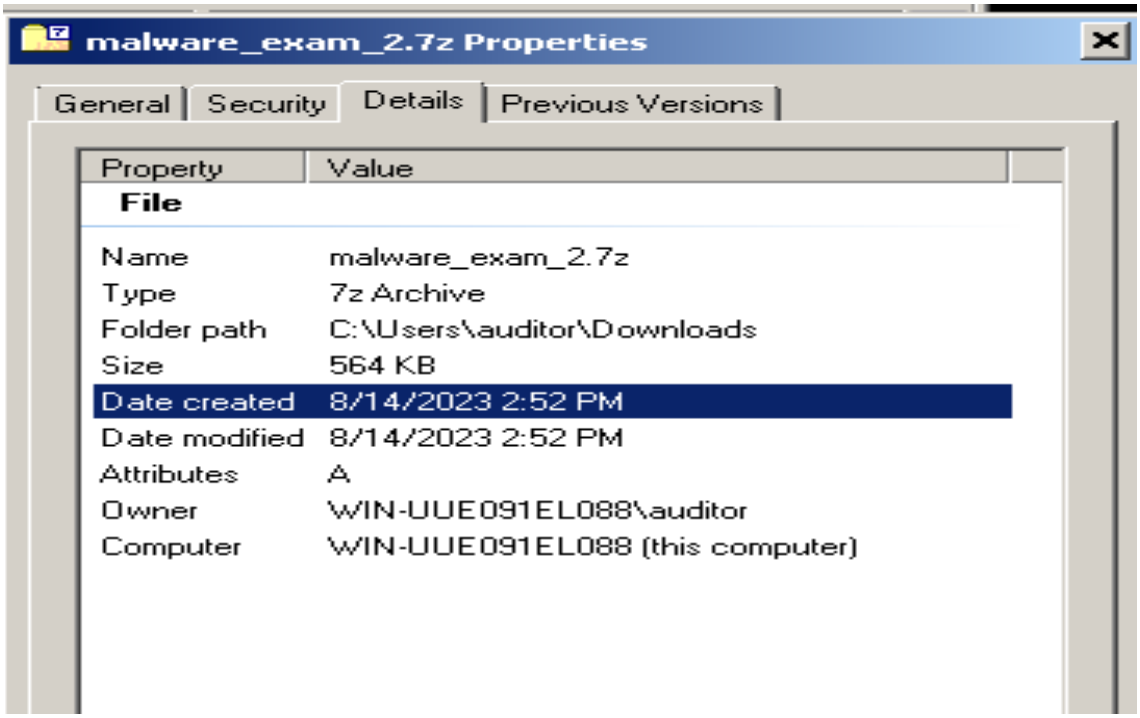
OSINT:

- Detection Scores: VirusTotal.com - 1/59



Metadata:

- Author, Company Name, Version are null when checked through using fie properties

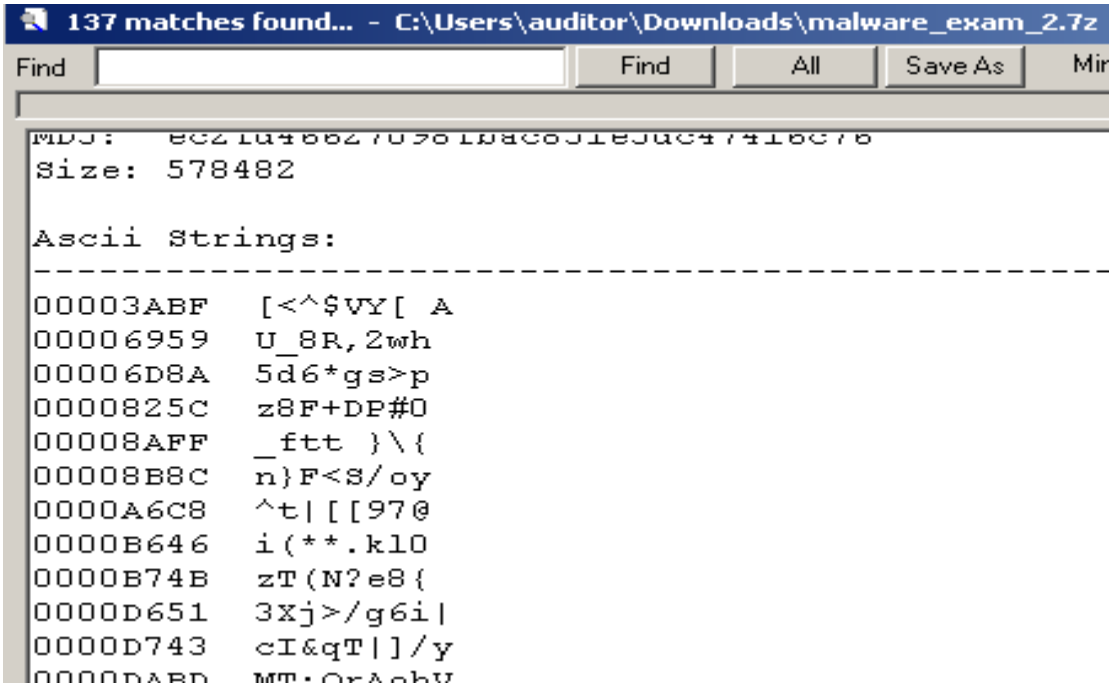


- Digital Signature (Authenticode): validity, signing company

Regarding the signature the information were empty and also the above image show cases the information provided through the host system but nothing specific regarding the creation of the malware.

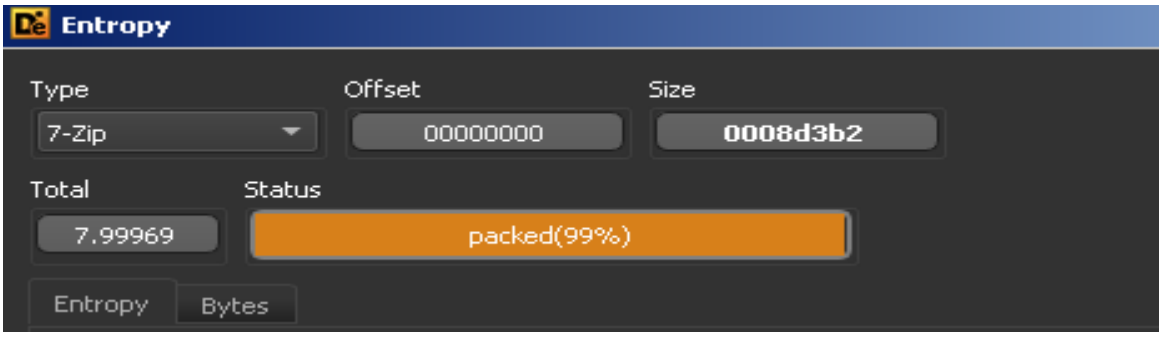
- File Type: Archive: 7-Zip(0.4) archived file according to the score of the virus total this raises a questioning of the major contents of the file and also the content must pack.

- Strings: the contents of the file are strongly obfuscated or compressed. Most of the strings information does not really help with further getting more helpful information. The below evidence is to record a proof of the string of this file.



-Entropy: 7.99969 99% packed by percentage the file is packed to 99% so the entropy is high

Ideally this evidence is lead analyzing strategy to the next part to realize the file is packed and its direct information it is a 7-zip file which should be further extracted in order to identify any executables and information relating to that.



- Portable Executable (PE) Structure:

The file is 7 zip and also gathering ay information related to this will be not ideal according to the stage so the information related to the PE structures will be investigated further

Solution and further step

Next step is to extract the file and doing another static analysis in order find more string information to gain more knowledge regarding the executable functions of the file having the malware

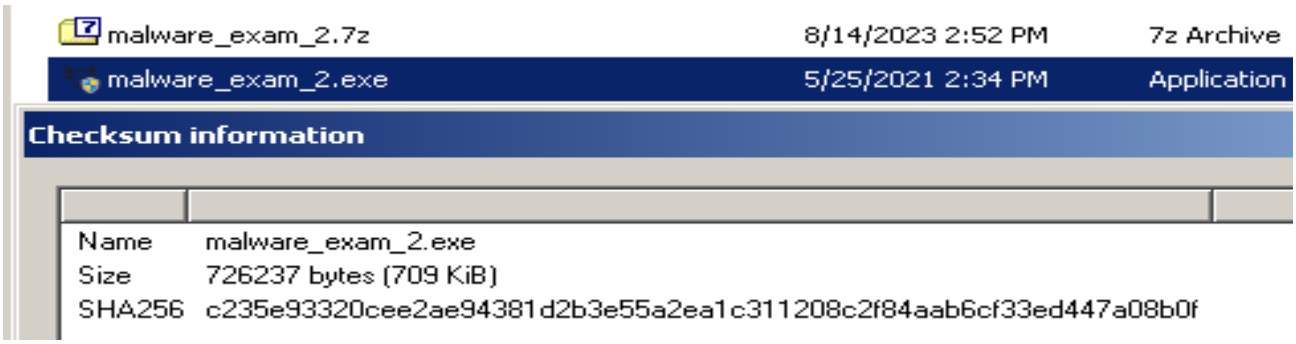
This stage has not yet contained any interesting facts but its more interesting as conclusion according to the result gain by the DETECT IT EASY which defined as so far the file contain more harmful content within inside the major file

2. Static analysis: malware_exam_2.exe

The following analysis made again on the extracted file of malware exam in this analysis since it is an exe file , and next steps of analyzing to further prove it as executable and also identify any suspicious function this file could do the system

File hash:

SHA-256 -c235e93320cee2ae94381d2b3e55a2ea1c311208c2f84aab6cf33ed447a08b0f

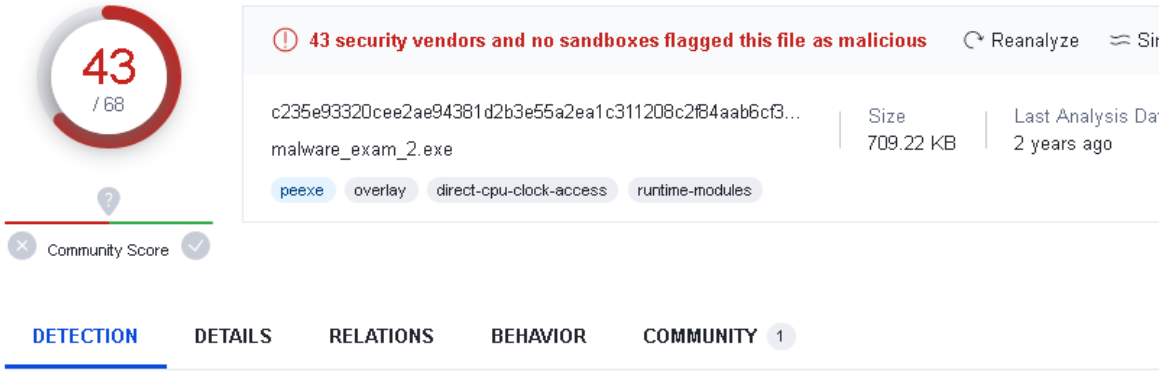


Again in order to compute the hash since its sha 256 at this stage better solution is to search any related incident related to this hash or move on to the next solution.

Since there were not any related result the analyzing will move to next information gathering.

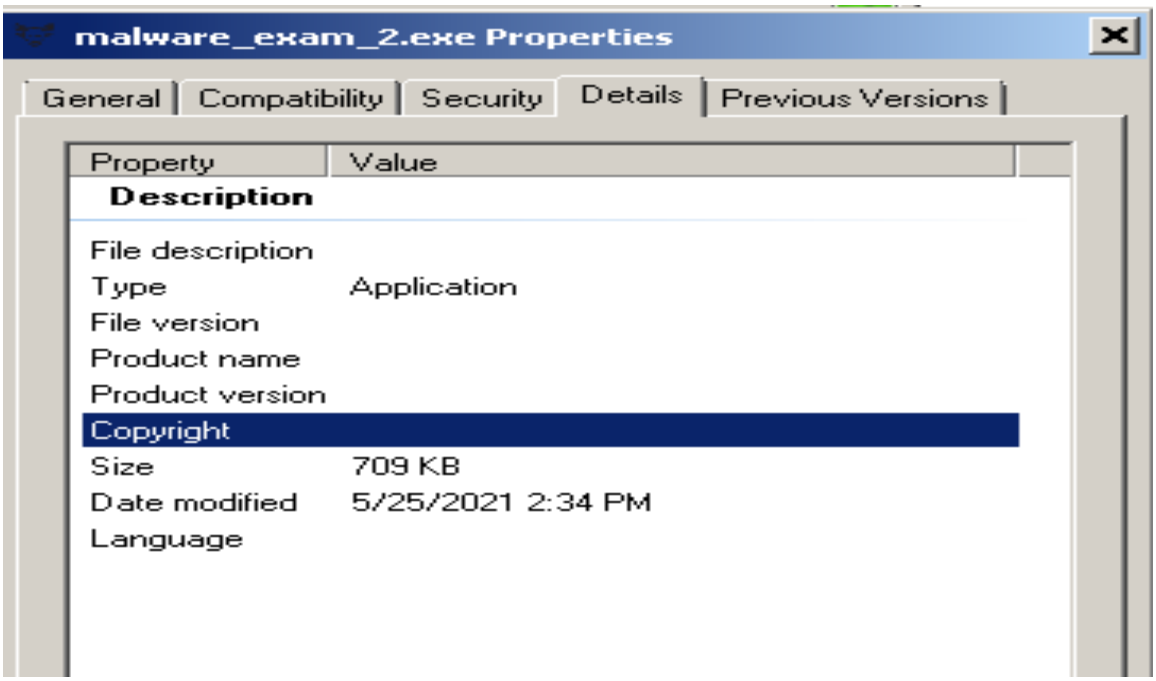
OSINT:

- Detection Scores: VirusTotal.com



After the file extracted the difference of the result of the same file providing more result and the score is to major threat level for the executable file.

Metadata:



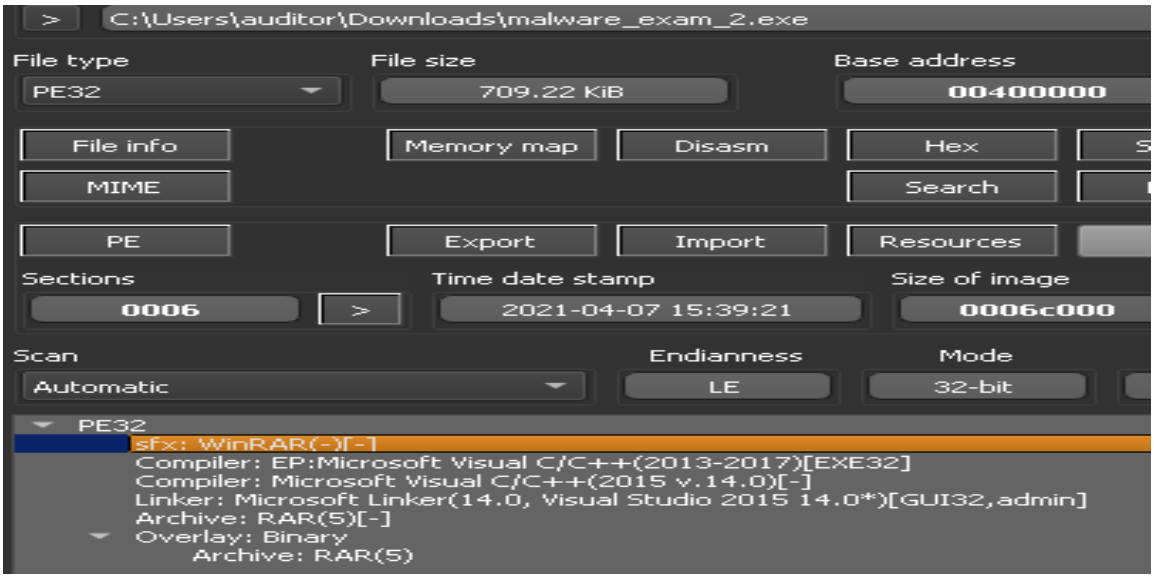
- Author, Company Name, Version

The above evidence significantly hides or do not provide the information or the identity of the source of the file this is not helpful and also much common in major malware files

- Digital Signature (Authenticode): validity, signing company,

Information related to digital signatures are null directly too when checked by the file properties

File Type: sfx WINRAR – the file is an auto launchable self-extracting file.

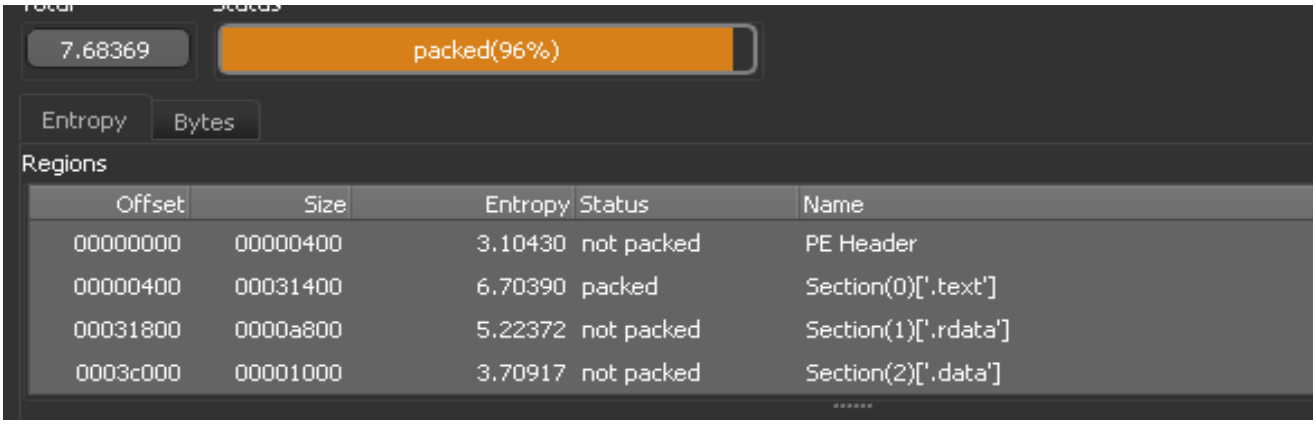


WinRAR sfx files will execute the file and run its function by self-extracting the further packed file within the parent file. In this malware content the suspicious matter in this stage is that the malware might contain further executable file within it which will run its functions step by step.

Strings: after extracting the strings of the malware not all are encrypted and was able to find pretty direct script written of sfx script. The script contains the function pushing two setup files under the program files and also contains the script which will kill process of the application its mentioned in the script.

```
00044E43  1 1$1(1,1014181<1@1D1H1L1P1T1X1\1`1d1h1p1t1x1|1
00045000  Rar!
0004502E  CMT;The comment below contains SFX script commands
00045064  Path=%appdata%\Program Files\
00045083  Setup="%appdata%\Program Files\$77_install.exe"
000450B4  Setup="%appdata%\Program Files\$77_svchost.exe"
000450E5  Presetup=taskkill /F /IM procexp.exe /IM procexp64.exe /IM procmon.exe /IM procmon64
/IM dnsquerysniffer.exe /IM processhacker.exe
0004516D  Presetup=cmd /c "echo Do you believe in all what you see?! > %tmp%\oups.txt"
000451BB  Presetup=cmd /c "start /b firefox.exe https://www.adeleda.com/?we_have_a_winner"
0004520D  Silent=1
00045217  Overwrite=2
00045224  License=
00045231  EPITA malware analysis exam
00045253  IiU-
0004526A  $77_svchost.exe
```

e. Entropy: 7.99969 99% packed



Offset	Size	Entropy	Status	Name
00000000	00000400	3.10430	not packed	PE Header
00000400	00031400	6.70390	packed	Section(0)['.text']
00031800	0000a800	5.22372	not packed	Section(1)['.rdata']
0003c000	00001000	3.70917	not packed	Section(2)['.data']

Portable Executable (PE) Structure:

The below evidence will show information's regarding the PE executable and structures of the file

```
PE32        Info        Comment   Text   Reload   Save

Info:
    File name: C:/Users/auditor/Downloads/malware_exam_2.exe
    Size: 726237(709.22 KiB)
    Operation system: Windows(XP)
    Architecture: I386
    Mode: 32-bit
    Type: GUI
    Endianness: LE
```

This contains the basic information regarding the executable file and also mainly its mentioned the architecture of the system and the mode

Simple it refers to the intel 80386 microprocessors which adds 32bit capabilities for the system.

Also the subsystem is Desktop since with the information of the system architecture

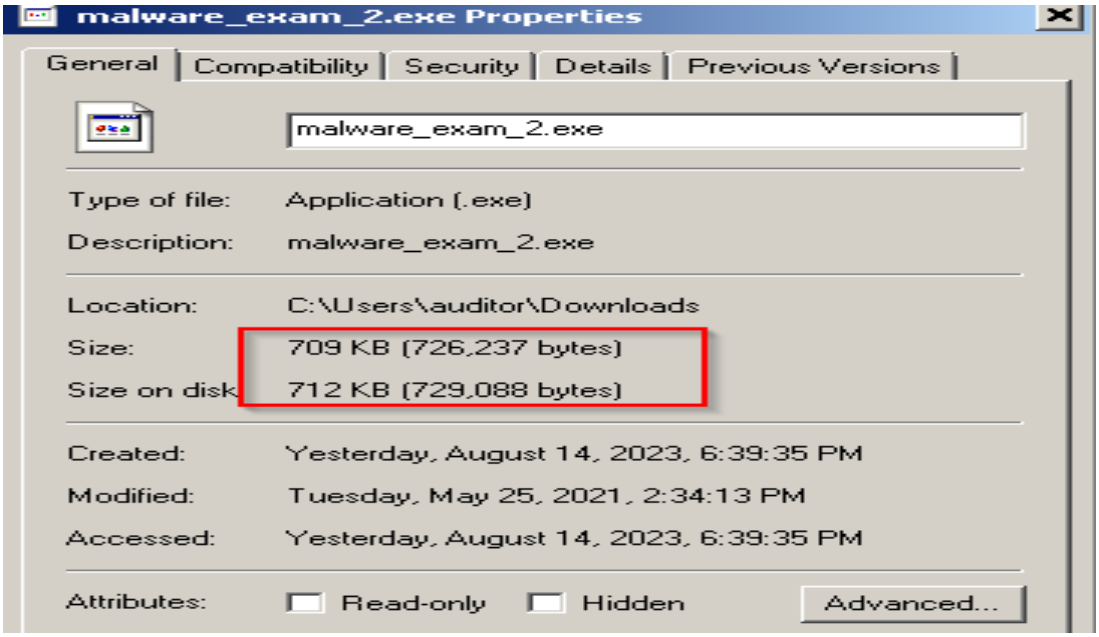
```
PE32        Entry point        Comment   Text   Reload

Entry point:
    Address: 0041ed60
    Offset: 0001e160
    Relative address: 0001ed60
    Bytes: e8a4040000e988feffff3b0d68e64300f27502f2c3f2e938060000cccccccc
    Signature: e8........e9........3b0d........f275..f2c3f2e9........cccccccc
    Signature(Rel): e8$$$$$$$$558bec83ec..8365....8365....a1........5657bf........
```

Entry Point of the target executable file- the information shows the point of instruction given when the application executes

Sections: contains the information of the section of the instructions code and its flags of each section also define each function of Read execute , read , read write all these functions when the application is executed

#	Name	Relative address	Virtual size	File offset	Size	Flags	Info
		00000000	00001000	00000000	00000400		Header
0	.text	00001000	0003122a	00000400	00031400	RE	(Compiler) Code Section
1	.rdata	00033000	0000a612	00031800	0000a800	R	(Compiler) Read-only initialized Data Section (MS ar
2	.data	0003e000	00023728	0003c000	00001000	RW	(Compiler) Data Section
3	.didat	00062000	00000188	0003d000	00000200	RW	(Compiler) Delay Import Section
4	.rsrc	00063000	000059e8	0003d200	00005a00	R	(Compiler) Resource section
5	.reloc	00069000	00002274	00042c00	00002400	R	(Compiler) Relocations Section
				00045000	0006c4dd		Overlay

anomalies: size on disk vs memory



- Imported APIs:

#	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk	Hash	Name
0	0003c890	00000000	00000000	0003d1d6	00033000	047c135b	KERNEL32.dll
1	0003cac8	00000000	00000000	0003d2a2	00033238	4671031c	gdiplus.dll

Exported APIs: functions that the software is exporting (seen in DLLs)

Name	Offset	Type	Value	
Characteristics	0000	DWORD	00000000	
TimeDateStamp	0004	DWORD	606dc419	2021-04-07 15:39:21
MajorVersion	0008	WORD	0000	
MinorVersion	000a	WORD	0000	
Name	000c	DWORD	0003c848	Hex sfxrar.exe
Base	0010	DWORD	00000001	
NumberOfFunctions	0014	DWORD	00000000	

Show valid

Above information is gathered in the part of static analysis in order to know all the functions and structure of application before running or executing in the system.

Next step will move towards on the dynamic analysis to run the executable and follow its functions and the behavior of the malware.

3. Dynamic analysis: malware_exam_2.exe

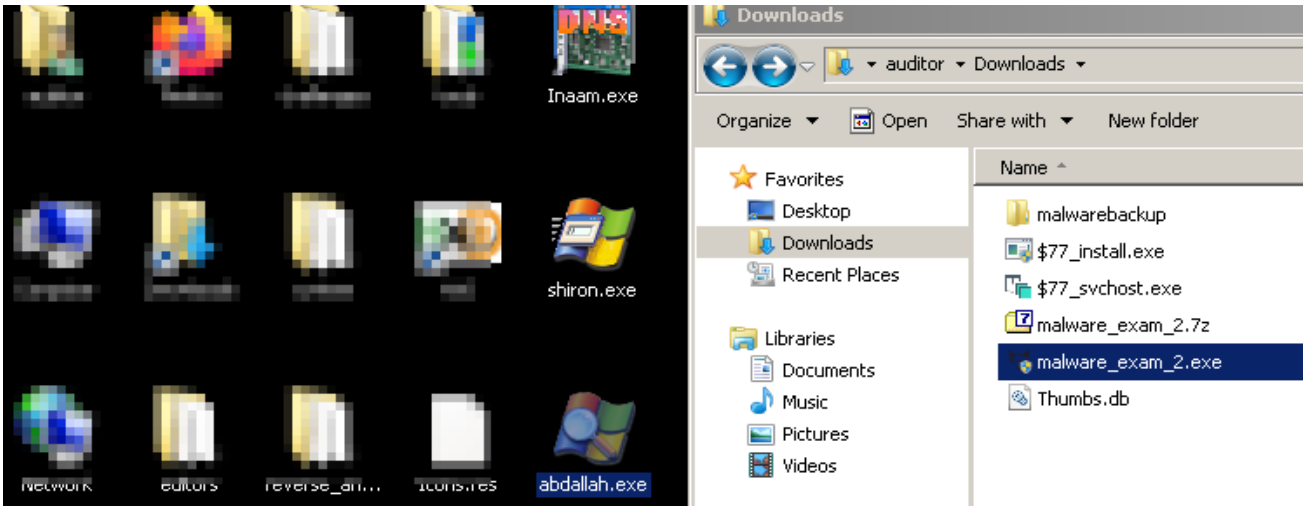
Virtual Machine + Operating System:

The operating system target for this analysis is the win 7 operating system in the virtual environment.

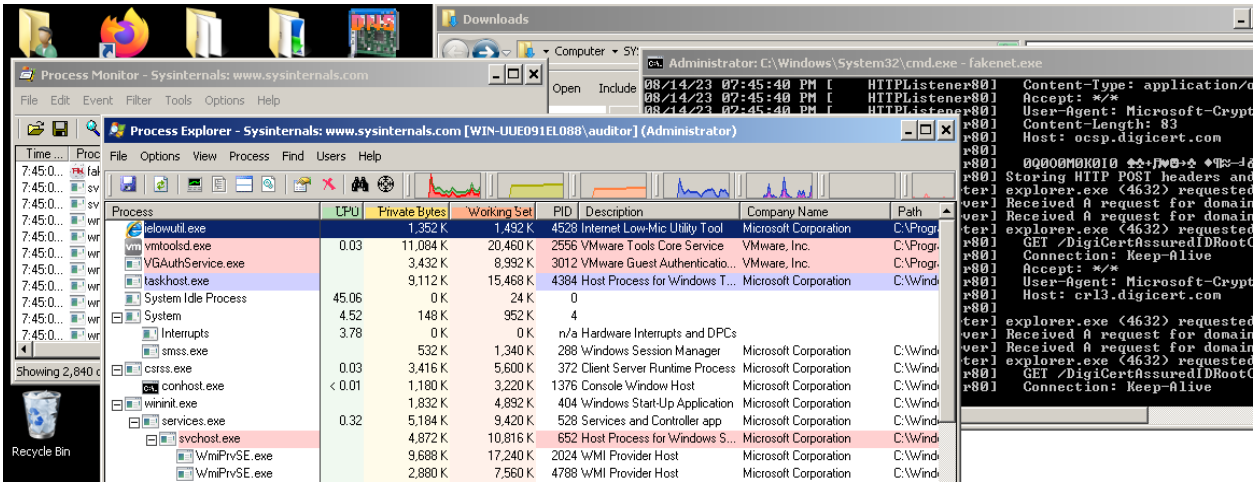
Customized OS: the operating system is customized in order to investigate any suspicious and threat-based files and activities related to the files.

With the above information from static gathered the further analysis and steps will be documented from the results of the dynamic results

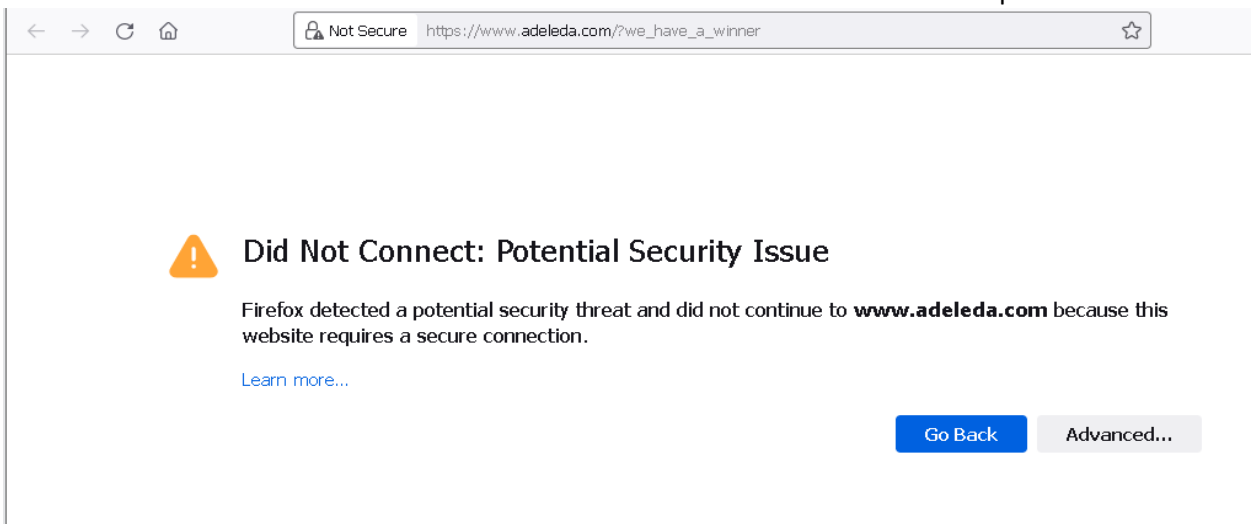
The step 1 – the awareness of the executable application and the script is known so because of that if the malware is executed with the processes application it will definitely kill all the process so by executing in both style the team tried by renaming the application mentioned in the script and execute the malware.



Next step will the evidence of the major process run during the investigation.



the evidence of the malware executed and its last function which redirect to the suspicious site



Did Not Connect: Potential Security Issue

Firefox detected a potential security threat and did not continue to **www.adeleda.com** because this website requires a secure connection.

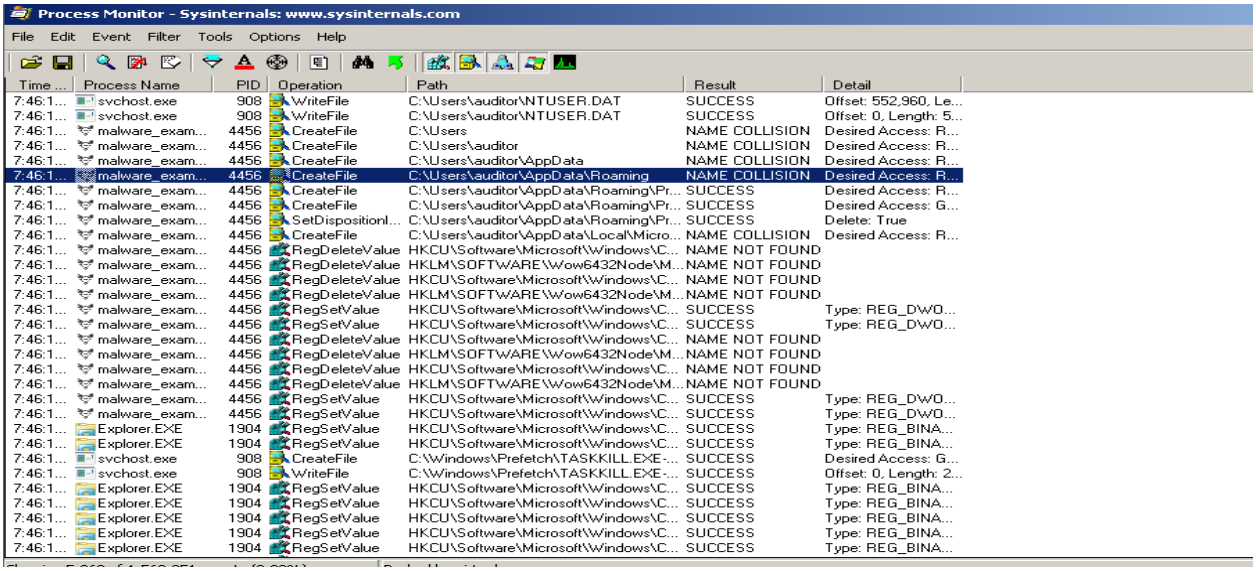
The understanding of the script during the analysis is that it does not identify the application it is just identify the names of the processes which was mentioned in the code.

Major application was used during the analysis was process explorer , process monitor and fake net

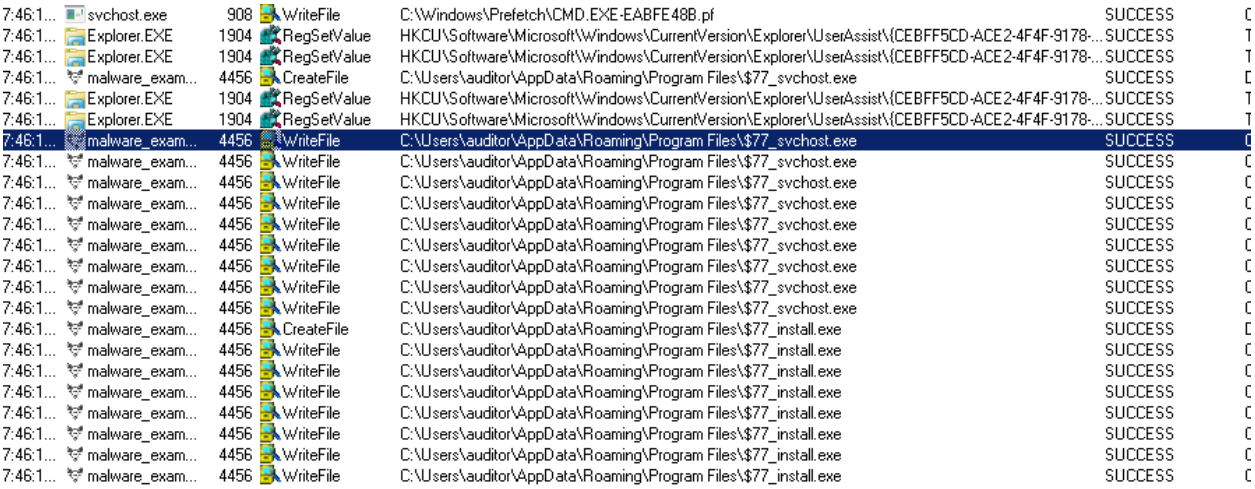
The usage of fake net was helpful to protect the communication to internet and helped the analysis further smoothly without more noises.

The results from the analysis and functions of the malware

Process monitor : process monitor



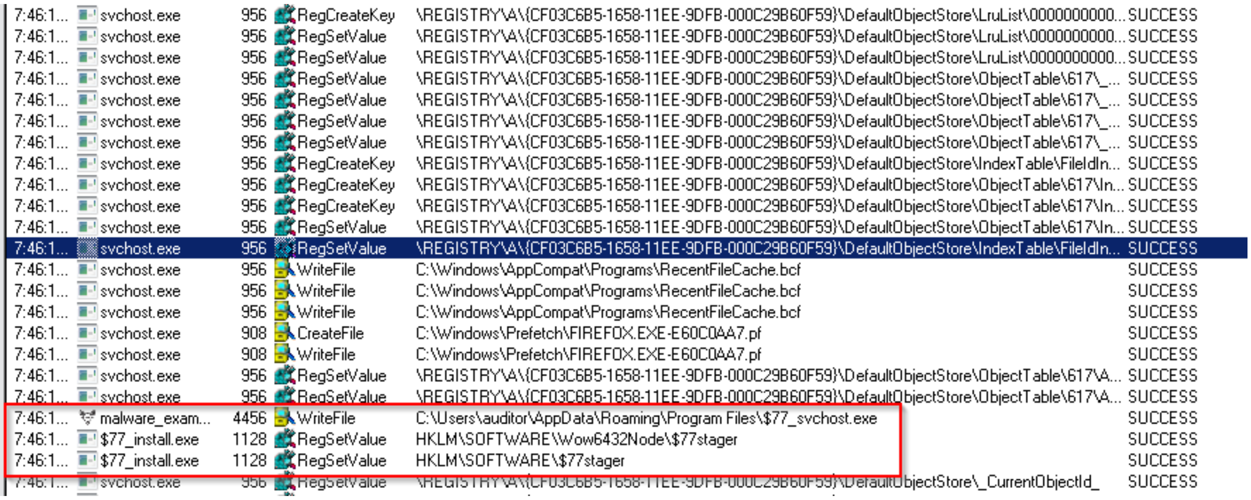
Time ...	Process Name	PID	Operation	Path	Result	Detail
7:46:1...	svchost.exe	908	WriteFile	C:\Users\auditor\NTUSER.DAT	SUCCESS	Offset: 552,960, Le...
7:46:1...	svchost.exe	908	WriteFile	C:\Users\auditor\NTUSER.DAT	SUCCESS	Offset: 0, Length: 5...
7:46:1...	malware_exam...	4456	CreateFile	C:\Users	NAME COLLISION	Desired Access: R...
7:46:1...	malware_exam...	4456	CreateFile	C:\Users\auditor	NAME COLLISION	Desired Access: R...
7:46:1...	malware_exam...	4456	CreateFile	C:\Users\auditor\AppData	NAME COLLISION	Desired Access: R...
7:46:1...	malware_exam...	4456	CreateFile	C:\Users\auditor\AppData\Roaming	NAME COLLISION	Desired Access: R...
7:46:1...	malware_exam...	4456	CreateFile	C:\Users\auditor\AppData\Roaming\Pr...	SUCCESS	Desired Access: R...
7:46:1...	malware_exam...	4456	CreateFile	C:\Users\auditor\AppData\Roaming\Pr...	SUCCESS	Desired Access: G...
7:46:1...	malware_exam...	4456	SetDispositionI...	C:\Users\auditor\AppData\Roaming\Pr...	SUCCESS	Delete: True
7:46:1...	malware_exam...	4456	CreateFile	C:\Users\auditor\AppData\Local\Micro...	NAME COLLISION	Desired Access: R...
7:46:1...	malware_exam...	4456	RegDeleteValue	HKCU\Software\Microsoft\Windows\C...	NAME NOT FOUND	
7:46:1...	malware_exam...	4456	RegDeleteValue	HKLM\SOFTWARE\Wow6432Node\M...	NAME NOT FOUND	
7:46:1...	malware_exam...	4456	RegDeleteValue	HKCU\Software\Microsoft\Windows\C...	NAME NOT FOUND	
7:46:1...	malware_exam...	4456	RegDeleteValue	HKLM\SOFTWARE\Wow6432Node\M...	NAME NOT FOUND	
7:46:1...	malware_exam...	4456	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_DWO...
7:46:1...	malware_exam...	4456	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_DWO...
7:46:1...	malware_exam...	4456	RegDeleteValue	HKCU\Software\Microsoft\Windows\C...	NAME NOT FOUND	
7:46:1...	malware_exam...	4456	RegDeleteValue	HKLM\SOFTWARE\Wow6432Node\M...	NAME NOT FOUND	
7:46:1...	malware_exam...	4456	RegDeleteValue	HKCU\Software\Microsoft\Windows\C...	NAME NOT FOUND	
7:46:1...	malware_exam...	4456	RegDeleteValue	HKLM\SOFTWARE\Wow6432Node\M...	NAME NOT FOUND	
7:46:1...	malware_exam...	4456	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_DWO...
7:46:1...	malware_exam...	4456	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_DWO...
7:46:1...	Explorer.EXE	1904	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_BINA...
7:46:1...	Explorer.EXE	1904	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_BINA...
7:46:1...	svchost.exe	908	CreateFile	C:\Windows\Prefetch\TASKKILL.EXE-...	SUCCESS	Desired Access: G...
7:46:1...	svchost.exe	908	WriteFile	C:\Windows\Prefetch\TASKKILL.EXE-...	SUCCESS	Offset: 0, Length: 2...
7:46:1...	Explorer.EXE	1904	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_BINA...
7:46:1...	Explorer.EXE	1904	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_BINA...
7:46:1...	Explorer.EXE	1904	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_BINA...
7:46:1...	Explorer.EXE	1904	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_BINA...
7:46:1...	Explorer.EXE	1904	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_BINA...



```
7:46:1...  svchost.exe      908  WriteFile    C:\Windows\Prefetch\CMD.EXE-EABFE48B.pf                                                       SUCCESS
7:46:1...  Explorer.EXE    1904  RegSetValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-...SUCCESS
7:46:1...  Explorer.EXE    1904  RegSetValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-...SUCCESS
7:46:1...  malware_exam... 4456  CreateFile   C:\Users\auditor\AppData\Roaming\Program Files\$77_svchost.exe                                SUCCESS
7:46:1...  Explorer.EXE    1904  RegSetValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-...SUCCESS
7:46:1...  Explorer.EXE    1904  RegSetValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-...SUCCESS
7:46:1...  malware_exam... 4456  WriteFile    C:\Users\auditor\AppData\Roaming\Program Files\$77_svchost.exe                                SUCCESS
7:46:1...  malware_exam... 4456  WriteFile    C:\Users\auditor\AppData\Roaming\Program Files\$77_svchost.exe                                SUCCESS
7:46:1...  malware_exam... 4456  WriteFile    C:\Users\auditor\AppData\Roaming\Program Files\$77_svchost.exe                                SUCCESS
7:46:1...  malware_exam... 4456  WriteFile    C:\Users\auditor\AppData\Roaming\Program Files\$77_svchost.exe                                SUCCESS
7:46:1...  malware_exam... 4456  WriteFile    C:\Users\auditor\AppData\Roaming\Program Files\$77_svchost.exe                                SUCCESS
7:46:1...  malware_exam... 4456  WriteFile    C:\Users\auditor\AppData\Roaming\Program Files\$77_svchost.exe                                SUCCESS
7:46:1...  malware_exam... 4456  WriteFile    C:\Users\auditor\AppData\Roaming\Program Files\$77_svchost.exe                                SUCCESS
7:46:1...  malware_exam... 4456  WriteFile    C:\Users\auditor\AppData\Roaming\Program Files\$77_svchost.exe                                SUCCESS
7:46:1...  malware_exam... 4456  WriteFile    C:\Users\auditor\AppData\Roaming\Program Files\$77_svchost.exe                                SUCCESS
7:46:1...  malware_exam... 4456  CreateFile   C:\Users\auditor\AppData\Roaming\Program Files\$77_install.exe                                SUCCESS
7:46:1...  malware_exam... 4456  WriteFile    C:\Users\auditor\AppData\Roaming\Program Files\$77_install.exe                                SUCCESS
7:46:1...  malware_exam... 4456  WriteFile    C:\Users\auditor\AppData\Roaming\Program Files\$77_install.exe                                SUCCESS
7:46:1...  malware_exam... 4456  WriteFile    C:\Users\auditor\AppData\Roaming\Program Files\$77_install.exe                                SUCCESS
7:46:1...  malware_exam... 4456  WriteFile    C:\Users\auditor\AppData\Roaming\Program Files\$77_install.exe                                SUCCESS
7:46:1...  malware_exam... 4456  WriteFile    C:\Users\auditor\AppData\Roaming\Program Files\$77_install.exe                                SUCCESS
7:46:1...  malware_exam... 4456  WriteFile    C:\Users\auditor\AppData\Roaming\Program Files\$77_install.exe                                SUCCESS
7:46:1...  malware_exam... 4456  WriteFile    C:\Users\auditor\AppData\Roaming\Program Files\$77_install.exe                                SUCCESS
```

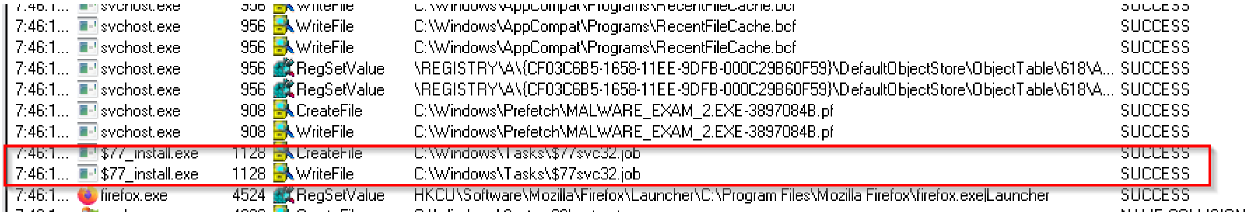
The above result indicates the function of malware as it is writing service svchost executable to the above location. The execution hidden the data or executable on the directory and keeps on automating the process.

Then the malware creates a install.exe file on the same directory to run its own function of the malware



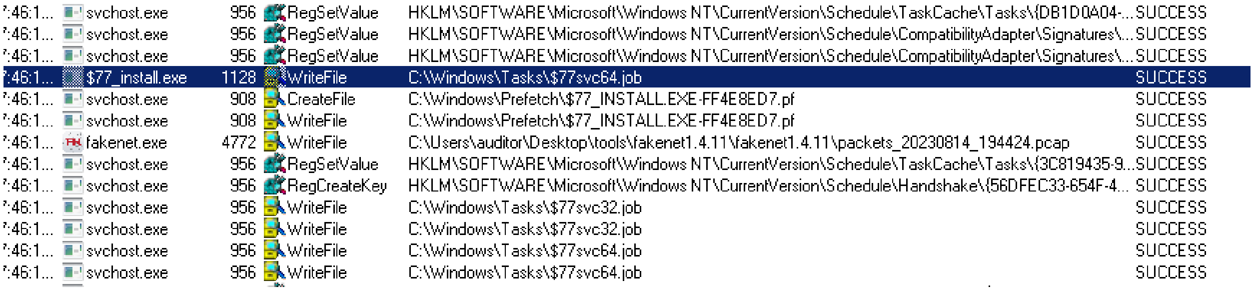
```
7:46:1...  svchost.exe       956  RegCreateKey  \REGISTRY\A\{CF03C6B5-1658-11EE-9DFB-000C29B60F59}\DefaultObjectStore\LruList\0000000000... SUCCESS
7:46:1...  svchost.exe       956  RegSetValue   \REGISTRY\A\{CF03C6B5-1658-11EE-9DFB-000C29B60F59}\DefaultObjectStore\LruList\0000000000... SUCCESS
7:46:1...  svchost.exe       956  RegSetValue   \REGISTRY\A\{CF03C6B5-1658-11EE-9DFB-000C29B60F59}\DefaultObjectStore\LruList\0000000000... SUCCESS
7:46:1...  svchost.exe       956  RegSetValue   \REGISTRY\A\{CF03C6B5-1658-11EE-9DFB-000C29B60F59}\DefaultObjectStore\ObjectTable\617\_...  SUCCESS
7:46:1...  svchost.exe       956  RegSetValue   \REGISTRY\A\{CF03C6B5-1658-11EE-9DFB-000C29B60F59}\DefaultObjectStore\ObjectTable\617\_...  SUCCESS
7:46:1...  svchost.exe       956  RegSetValue   \REGISTRY\A\{CF03C6B5-1658-11EE-9DFB-000C29B60F59}\DefaultObjectStore\ObjectTable\617\_...  SUCCESS
7:46:1...  svchost.exe       956  RegSetValue   \REGISTRY\A\{CF03C6B5-1658-11EE-9DFB-000C29B60F59}\DefaultObjectStore\ObjectTable\617\_...  SUCCESS
7:46:1...  svchost.exe       956  RegCreateKey  \REGISTRY\A\{CF03C6B5-1658-11EE-9DFB-000C29B60F59}\DefaultObjectStore\IndexTable\FileIdIn...  SUCCESS
7:46:1...  svchost.exe       956  RegCreateKey  \REGISTRY\A\{CF03C6B5-1658-11EE-9DFB-000C29B60F59}\DefaultObjectStore\ObjectTable\617\In...  SUCCESS
7:46:1...  svchost.exe       956  RegCreateKey  \REGISTRY\A\{CF03C6B5-1658-11EE-9DFB-000C29B60F59}\DefaultObjectStore\ObjectTable\617\In...  SUCCESS
7:46:1...  svchost.exe       956  RegSetValue   \REGISTRY\A\{CF03C6B5-1658-11EE-9DFB-000C29B60F59}\DefaultObjectStore\ObjectTable\617\In...  SUCCESS
7:46:1...  svchost.exe       956  RegSetValue   \REGISTRY\A\{CF03C6B5-1658-11EE-9DFB-000C29B60F59}\DefaultObjectStore\IndexTable\FileIdIn...  SUCCESS
7:46:1...  svchost.exe       956  WriteFile     C:\Windows\AppCompat\Programs\RecentFileCache.bcf                                          SUCCESS
7:46:1...  svchost.exe       956  WriteFile     C:\Windows\AppCompat\Programs\RecentFileCache.bcf                                          SUCCESS
7:46:1...  svchost.exe       956  WriteFile     C:\Windows\AppCompat\Programs\RecentFileCache.bcf                                          SUCCESS
7:46:1...  svchost.exe       908  CreateFile    C:\Windows\Prefetch\FIREFOX.EXE-E60C0AA7.pf                                                SUCCESS
7:46:1...  svchost.exe       908  WriteFile     C:\Windows\Prefetch\FIREFOX.EXE-E60C0AA7.pf                                                SUCCESS
7:46:1...  svchost.exe       956  RegSetValue   \REGISTRY\A\{CF03C6B5-1658-11EE-9DFB-000C29B60F59}\DefaultObjectStore\ObjectTable\617\A...  SUCCESS
7:46:1...  svchost.exe       956  RegSetValue   \REGISTRY\A\{CF03C6B5-1658-11EE-9DFB-000C29B60F59}\DefaultObjectStore\ObjectTable\617\A...  SUCCESS
7:46:1...  malware_exam...  4456  WriteFile     C:\Users\auditor\AppData\Roaming\Program Files\$77_svchost.exe                             SUCCESS
7:46:1...  $77_install.exe  1128  RegSetValue   HKLM\SOFTWARE\Wow6432Node\$77stager                                                        SUCCESS
7:46:1...  $77_install.exe  1128  RegSetValue   HKLM\SOFTWARE\$77stager                                                                    SUCCESS
7:46:1...  svchost.exe       956  RegSetValue   \REGISTRY\A\{CF03C6B5-1658-11EE-9DFB-000C29B60F59}\DefaultObjectStore\_CurrentObjectId_     SUCCESS
```

The above function of the behavior patter where the malware creates by writing the file inside the above location and under the install.exe its registers the stager or the payload in order to run its next functions of the script.



```
7:46:1...  svchost.exe       956  WriteFile    C:\Windows\AppCompat\Programs\RecentFileCache.bcf                                          SUCCESS
7:46:1...  svchost.exe       956  WriteFile    C:\Windows\AppCompat\Programs\RecentFileCache.bcf                                          SUCCESS
7:46:1...  svchost.exe       956  WriteFile    C:\Windows\AppCompat\Programs\RecentFileCache.bcf                                          SUCCESS
7:46:1...  svchost.exe       956  RegSetValue  \REGISTRY\A\{CF03C6B5-1658-11EE-9DFB-000C29B60F59}\DefaultObjectStore\ObjectTable\618\A...  SUCCESS
7:46:1...  svchost.exe       956  RegSetValue  \REGISTRY\A\{CF03C6B5-1658-11EE-9DFB-000C29B60F59}\DefaultObjectStore\ObjectTable\618\A...  SUCCESS
7:46:1...  svchost.exe       908  CreateFile   C:\Windows\Prefetch\MALWARE_EXAM_2.EXE-3897084B.pf                                         SUCCESS
7:46:1...  svchost.exe       908  WriteFile    C:\Windows\Prefetch\MALWARE_EXAM_2.EXE-3897084B.pf                                         SUCCESS
7:46:1...  $77_install.exe  1128  CreateFile   C:\Windows\Tasks\$77svc32.job                                                              SUCCESS
7:46:1...  $77_install.exe  1128  WriteFile    C:\Windows\Tasks\$77svc32.job                                                              SUCCESS
7:46:1...  firefox.exe      4524  RegSetValue  HKCU\Software\Mozilla\Firefox\Launcher\C:\Program Files\Mozilla Firefox\firefox.exe|Launcher SUCCESS
```

This targets the task files by hiding its functions according to the function of the execution malware

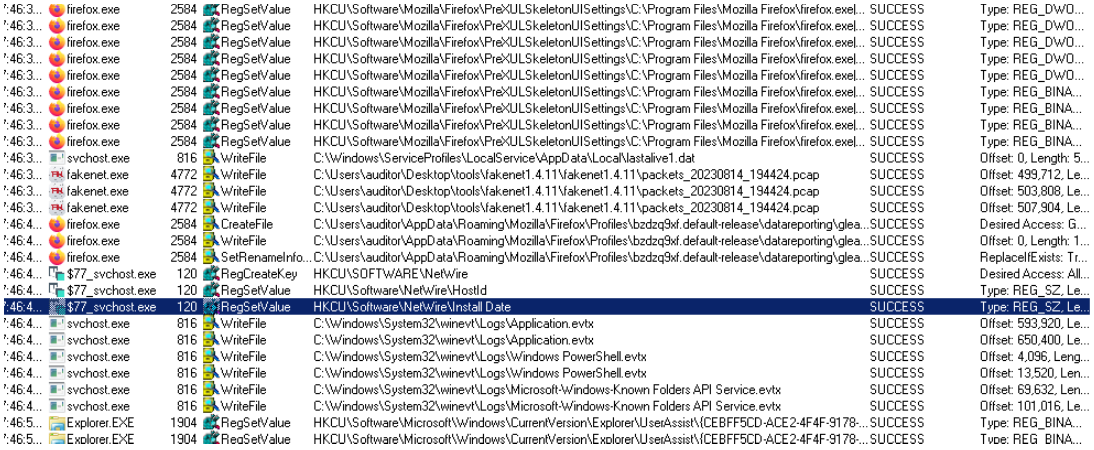


```
:46:1...  svchost.exe     956  RegSetValue   HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{DB1D0A04-...SUCCESS
:46:1...  svchost.exe     956  RegSetValue   HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\...SUCCESS
:46:1...  svchost.exe     956  RegSetValue   HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\...SUCCESS
:46:1...  $77_install.exe 1128 WriteFile     C:\Windows\Tasks\$77svc64.job                                                  SUCCESS
:46:1...  svchost.exe     908  CreateFile    C:\Windows\Prefetch\$77_INSTALL.EXE-FF4E8ED7.pf                                SUCCESS
:46:1...  svchost.exe     908  WriteFile     C:\Windows\Prefetch\$77_INSTALL.EXE-FF4E8ED7.pf                                SUCCESS
:46:1...  fakenet.exe     4772 WriteFile     C:\Users\auditor\Desktop\tools\fakenet1.4.11\fakenet1.4.11\packets_20230814_194424.pcap SUCCESS
:46:1...  svchost.exe     956  RegSetValue   HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{3C819435-9...SUCCESS
:46:1...  svchost.exe     956  RegCreateKey  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Handshake\{56DFEC33-654F-4... SUCCESS
:46:1...  svchost.exe     956  WriteFile     C:\Windows\Tasks\$77svc32.job                                                  SUCCESS
:46:1...  svchost.exe     956  WriteFile     C:\Windows\Tasks\$77svc32.job                                                  SUCCESS
:46:1...  svchost.exe     956  WriteFile     C:\Windows\Tasks\$77svc64.job                                                  SUCCESS
:46:1...  svchost.exe     956  WriteFile     C:\Windows\Tasks\$77svc64.job                                                  SUCCESS
```

It creates the prefetch file install.exe which manipulates with the run time execution or plays with the performance of the system how it runs the behavior and functions of the malware

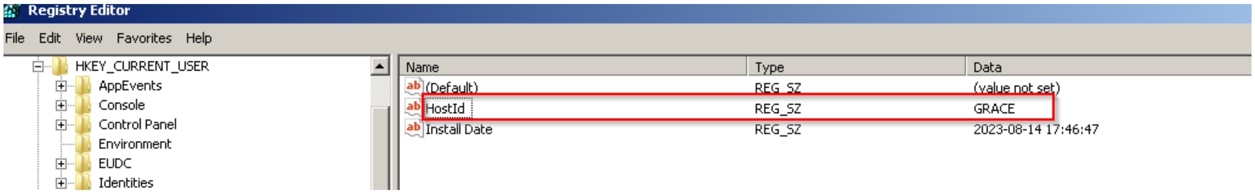
```
7:46:1...  explorer.exe    4632 CreateFile     C:\Windows\System32\catroot2                                                       NAME COLLISION
7:46:1...  powershell.EXE  2660 CreateFile     C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\Caches  NAME COLLISION
7:46:1...  powershell.EXE  2660 CreateFile     C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\Caches  NAME COLLISION
7:46:1...  powershell.EXE  2660 CreateFile     C:\Windows\system32\config\systemprofile\AppData\Roaming\Microsoft\Windows\Recent\CustomDe... PATH NOT FOUN
7:46:1...  powershell.EXE  2660 CreateFile     C:\Windows\system32\config\systemprofile\AppData\Roaming\Microsoft\Windows\Recent\CustomDe... PATH NOT FOUN
7:46:1...  svchost.exe     908  CreateFile     C:\Windows\Prefetch\DLLHOST.EXE-893DDF55.pf                                       SUCCESS
7:46:1...  svchost.exe     908  WriteFile      C:\Windows\Prefetch\DLLHOST.EXE-893DDF55.pf                                       SUCCESS
7:46:1...  powershell.EXE  2660 CreateFile     C:\Windows\System32\config\systemprofile                                          NAME COLLISION
7:46:1...  powershell.EXE  2660 CreateFile     C:\Windows\System32\config\systemprofile\AppData\Roaming                         NAME COLLISION
7:46:1...  firefox.exe     2584 SetRenameInfo... C:\Users\auditor\AppData\Roaming\Mozilla\Firefox\Profiles\bzdzq9xf.default-release\sessionstore-back... SUCCESS
7:46:1...  firefox.exe     2584 CreateFile     C:\Users\auditor\AppData\Roaming\Mozilla\Firefox\Profiles\bzdzq9xf.default-release\sessionstore-back... NAME COLLISION
7:46:1...  firefox.exe     2584 CreateFile     C:\Users\auditor\AppData\Roaming\Mozilla\Firefox\Profiles\bzdzq9xf.default-release\sessionstore-back... SUCCESS
7:46:1...  firefox.exe     2584 WriteFile      C:\Users\auditor\AppData\Roaming\Mozilla\Firefox\Profiles\bzdzq9xf.default-release\sessionstore-back... SUCCESS
7:46:1     firefox.exe     2584 SetRenameInfo  C:\Users\auditor\AppData\Roaming\Mozilla\Firefox\Profiles\bzdzq9xf.default-release\sessionstore-back SUCCESS
7:46:1...  dllhost.exe     3544 RegCreateKey   HKLM\SOFTWARE\$77config                                                           SUCCESS
7:46:1...  dllhost.exe     3544 RegCreateKey   HKLM\SOFTWARE\$77config\pid                                                       SUCCESS
7:46:1...  dllhost.exe     3544 RegSetValue    HKLM\SOFTWARE\$77config\pid\svc32                                                 SUCCESS
7:46:1...  svchost.exe     908  CreateFile     C:\Windows\Prefetch\POWERSHELL.EXE-3E7086C1.pf                                    SUCCESS
7:46:1...  svchost.exe     908  WriteFile      C:\Windows\Prefetch\POWERSHELL.EXE-3E7086C1.pf                                    SUCCESS
7:46:1...  svchost.exe     908  CreateFile     C:\Windows\Prefetch\CONHOST.EXE-3218E401.pf                                       SUCCESS
7:46:1...  svchost.exe     908  WriteFile      C:\Windows\Prefetch\CONHOST.EXE-3218E401.pf                                       SUCCESS
7:46:1...  svchost.exe     956  RegSetValue    HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{3C819435-9...SUCCESS
7:46:1...  svchost.exe     908  CreateFile     C:\Windows\Prefetch\POWERSHELL.EXE-59FC8F3D.pf                                    SUCCESS
7:46:1...  svchost.exe     908  WriteFile      C:\Windows\Prefetch\POWERSHELL.EXE-59FC8F3D.pf                                    SUCCESS
7:46:1...  svchost.exe     908  CreateFile     C:\Windows\Prefetch\CONHOST.EXE-3218E401.pf                                       SUCCESS
7:46:1...  svchost.exe     908  WriteFile      C:\Windows\Prefetch\CONHOST.EXE-3218E401.pf                                       SUCCESS
7:46:1     svchost.exe     956  RegSetValue    HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{DB1D0A04- SUCCESS
7:46:1...  dllhost.exe     316  RegSetValue    HKLM\SOFTWARE\$77config\pid\svc64                                                 SUCCESS
```

Now the malware targets the registry by installing its config file on the HKLM registry through dllhost.exe which is the function responsible for running most of its resources of the system performance. The malware is hiding the registry of the config file under this.



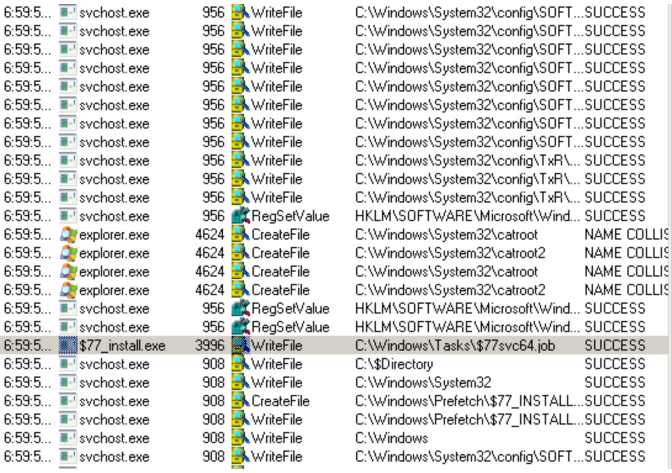
```
:46:3...  firefox.exe      2584 RegSetValue     HKCU\Software\Mozilla\Firefox\PreXULSkeletonUISettings\C:\Program Files\Mozilla Firefox\firefox.exe|... SUCCESS  Type: REG_DWO...
:46:3...  firefox.exe      2584 RegSetValue     HKCU\Software\Mozilla\Firefox\PreXULSkeletonUISettings\C:\Program Files\Mozilla Firefox\firefox.exe|... SUCCESS  Type: REG_DWO...
:46:3...  firefox.exe      2584 RegSetValue     HKCU\Software\Mozilla\Firefox\PreXULSkeletonUISettings\C:\Program Files\Mozilla Firefox\firefox.exe|... SUCCESS  Type: REG_DWO...
:46:3...  firefox.exe      2584 RegSetValue     HKCU\Software\Mozilla\Firefox\PreXULSkeletonUISettings\C:\Program Files\Mozilla Firefox\firefox.exe|... SUCCESS  Type: REG_DWO...
:46:3...  firefox.exe      2584 RegSetValue     HKCU\Software\Mozilla\Firefox\PreXULSkeletonUISettings\C:\Program Files\Mozilla Firefox\firefox.exe|... SUCCESS  Type: REG_DWO...
:46:3...  firefox.exe      2584 RegSetValue     HKCU\Software\Mozilla\Firefox\PreXULSkeletonUISettings\C:\Program Files\Mozilla Firefox\firefox.exe|... SUCCESS  Type: REG_BINA...
:46:3...  firefox.exe      2584 RegSetValue     HKCU\Software\Mozilla\Firefox\PreXULSkeletonUISettings\C:\Program Files\Mozilla Firefox\firefox.exe|... SUCCESS  Type: REG_BINA...
:46:3...  firefox.exe      2584 RegSetValue     HKCU\Software\Mozilla\Firefox\PreXULSkeletonUISettings\C:\Program Files\Mozilla Firefox\firefox.exe|... SUCCESS  Type: REG_BINA...
:46:3...  firefox.exe      2584 RegSetValue     HKCU\Software\Mozilla\Firefox\PreXULSkeletonUISettings\C:\Program Files\Mozilla Firefox\firefox.exe|... SUCCESS  Type: REG_BINA...
:46:3...  svchost.exe      816  WriteFile       C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive1.dat                              SUCCESS  Offset: 0, Length: 5...
:46:3...  fakenet.exe      4772 WriteFile       C:\Users\auditor\Desktop\tools\fakenet1.4.11\fakenet1.4.11\packets_20230814_194424.pcap           SUCCESS  Offset: 499,712, Le...
:46:3...  fakenet.exe      4772 WriteFile       C:\Users\auditor\Desktop\tools\fakenet1.4.11\fakenet1.4.11\packets_20230814_194424.pcap           SUCCESS  Offset: 503,808, Le...
:46:3...  fakenet.exe      4772 WriteFile       C:\Users\auditor\Desktop\tools\fakenet1.4.11\fakenet1.4.11\packets_20230814_194424.pcap           SUCCESS  Offset: 507,904, Le...
:46:4...  firefox.exe      2584 CreateFile      C:\Users\auditor\AppData\Roaming\Mozilla\Firefox\Profiles\bzdzq9xf.default-release\datareporting\glea...SUCCESS  Desired Access: G...
:46:4...  firefox.exe      2584 WriteFile       C:\Users\auditor\AppData\Roaming\Mozilla\Firefox\Profiles\bzdzq9xf.default-release\datareporting\glea...SUCCESS  Offset: 0, Length: 1...
:46:4...  firefox.exe      2584 SetRenameInfo... C:\Users\auditor\AppData\Roaming\Mozilla\Firefox\Profiles\bzdzq9xf.default-release\datareporting\glea...SUCCESS  ReplaceIfExists: Tr...
:46:4...  $77_svchost.exe  120  RegCreateKey    HKCU\SOFTWARE\NetWire                                                                             SUCCESS  Desired Access: All...
:46:4...  $77_svchost.exe  120  RegSetValue     HKCU\Software\NetWire\HostId                                                                      SUCCESS  Type: REG_SZ, Le...
:46:4...  $77_svchost.exe  120  RegSetValue     HKCU\Software\NetWire\Install Date                                                                SUCCESS  Type: REG_SZ, Le...
:46:4...  svchost.exe      816  WriteFile       C:\Windows\System32\winevt\Logs\Application.evtx                                                  SUCCESS  Offset: 593,920, Le...
:46:4...  svchost.exe      816  WriteFile       C:\Windows\System32\winevt\Logs\Application.evtx                                                  SUCCESS  Offset: 650,400, Le...
:46:4...  svchost.exe      816  WriteFile       C:\Windows\System32\winevt\Logs\Windows PowerShell.evtx                                           SUCCESS  Offset: 4,096, Leng...
:46:4...  svchost.exe      816  WriteFile       C:\Windows\System32\winevt\Logs\Windows PowerShell.evtx                                           SUCCESS  Offset: 13,520, Len...
:46:4...  svchost.exe      816  WriteFile       C:\Windows\System32\winevt\Logs\Microsoft-Windows-Known Folders API Service.evtx                  SUCCESS  Offset: 69,632, Len...
:46:4...  svchost.exe      816  WriteFile       C:\Windows\System32\winevt\Logs\Microsoft-Windows-Known Folders API Service.evtx                  SUCCESS  Offset: 101,016, Le...
:46:5...  Explorer.EXE     1904 RegSetValue     HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-...SUCCESS  Type: REG_BINA...
:46:5...  Explorer.EXE     1904 RegSetValue     HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-...SUCCESS  Type: REG_BINA...
```

Under HK current user by using the svchost it creates the host ID and install date

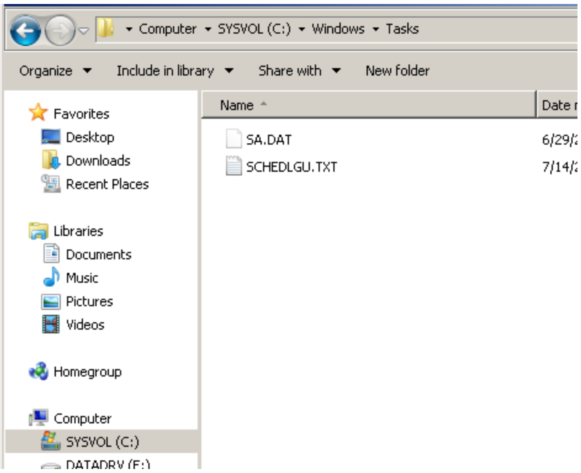


Name	Type	Data
(Default)	REG_SZ	(value not set)
HostId	REG_SZ	GRACE
Install Date	REG_SZ	2023-08-14 17:46:47

Evidence of the registry file of installing the host ID and date is exactly matches the execution time of the malware.



```
6:59:5... svchost.exe     956  WriteFile    C:\Windows\System32\config\SOFT...SUCCESS
6:59:5... svchost.exe     956  WriteFile    C:\Windows\System32\config\SOFT...SUCCESS
6:59:5... svchost.exe     956  WriteFile    C:\Windows\System32\config\SOFT...SUCCESS
6:59:5... svchost.exe     956  WriteFile    C:\Windows\System32\config\SOFT...SUCCESS
6:59:5... svchost.exe     956  WriteFile    C:\Windows\System32\config\SOFT...SUCCESS
6:59:5... svchost.exe     956  WriteFile    C:\Windows\System32\config\SOFT...SUCCESS
6:59:5... svchost.exe     956  WriteFile    C:\Windows\System32\config\SOFT...SUCCESS
6:59:5... svchost.exe     956  WriteFile    C:\Windows\System32\config\SOFT...SUCCESS
6:59:5... svchost.exe     956  WriteFile    C:\Windows\System32\config\TxR\... SUCCESS
6:59:5... svchost.exe     956  WriteFile    C:\Windows\System32\config\TxR\... SUCCESS
6:59:5... svchost.exe     956  WriteFile    C:\Windows\System32\config\TxR\... SUCCESS
6:59:5... svchost.exe     956  RegSetValue  HKLM\SOFTWARE\Microsoft\Wind... SUCCESS
6:59:5... explorer.exe   4624  CreateFile   C:\Windows\System32\catroot       NAME COLLIS
6:59:5... explorer.exe   4624  CreateFile   C:\Windows\System32\catroot2      NAME COLLIS
6:59:5... explorer.exe   4624  CreateFile   C:\Windows\System32\catroot       NAME COLLIS
6:59:5... explorer.exe   4624  CreateFile   C:\Windows\System32\catroot2      NAME COLLIS
6:59:5... svchost.exe     956  RegSetValue  HKLM\SOFTWARE\Microsoft\Wind... SUCCESS
6:59:5... svchost.exe     956  RegSetValue  HKLM\SOFTWARE\Microsoft\Wind... SUCCESS
6:59:5... $77_install.exe 3996 WriteFile    C:\Windows\Tasks\$77svc64.job     SUCCESS
6:59:5... svchost.exe     908  WriteFile    C:\$Directory                     SUCCESS
6:59:5... svchost.exe     908  WriteFile    C:\Windows\System32               SUCCESS
6:59:5... svchost.exe     908  CreateFile   C:\Windows\Prefetch\$77_INSTALL...SUCCESS
6:59:5... svchost.exe     908  WriteFile    C:\Windows\Prefetch\$77_INSTALL...SUCCESS
6:59:5... svchost.exe     908  WriteFile    C:\Windows                        SUCCESS
6:59:5... svchost.exe     908  WriteFile    C:\Windows\System32\config\SOFT...SUCCESS
```



Name	Date r
SA.DAT	6/29/
SCHEDLGU.TXT	7/14/

By checking both function and folder or the location where function writes to is clearly explained the malware has its own type of behavior and its objective after it gets executed

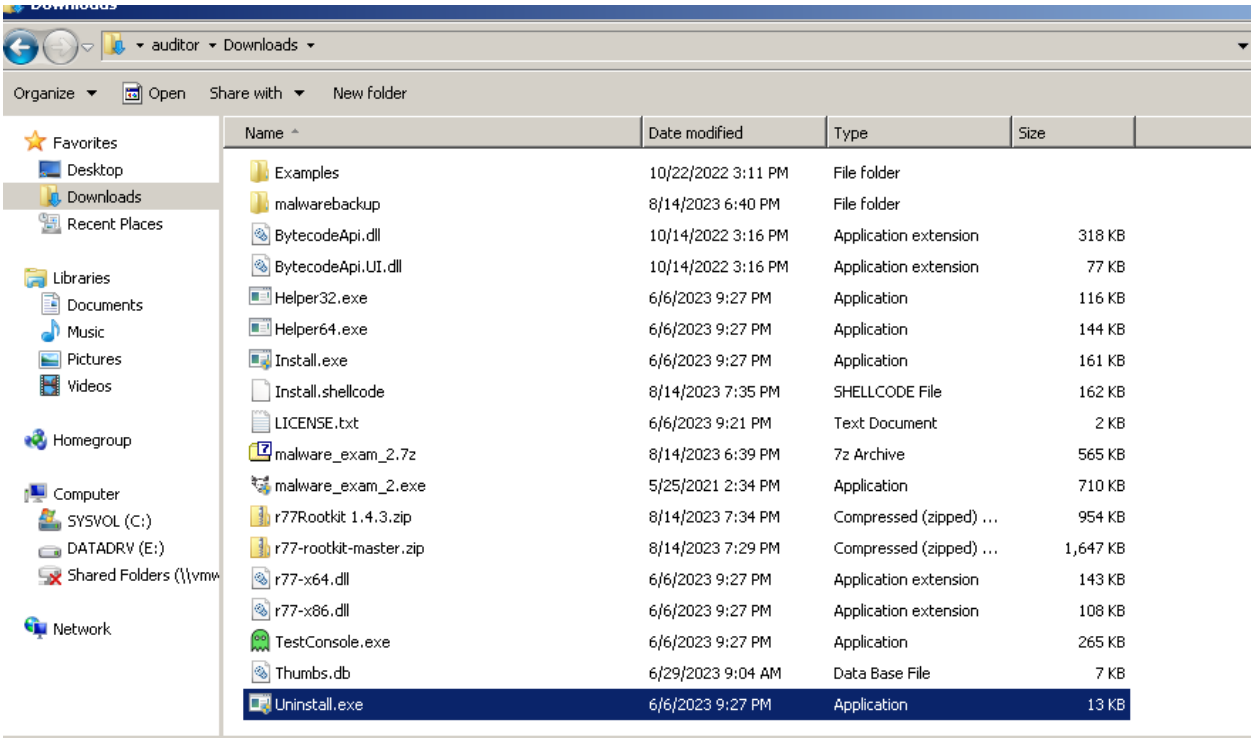
Major note of the malware function captures by process monitor is the $77 sign then analyze part moved on to research method to identify the type of the malware and what it does.

For the findings it was proved that the type of malware was executed is **r77 rootkit** which ideally hides everything including registries, directories , services even scheduled task above according to this specific rootkit.

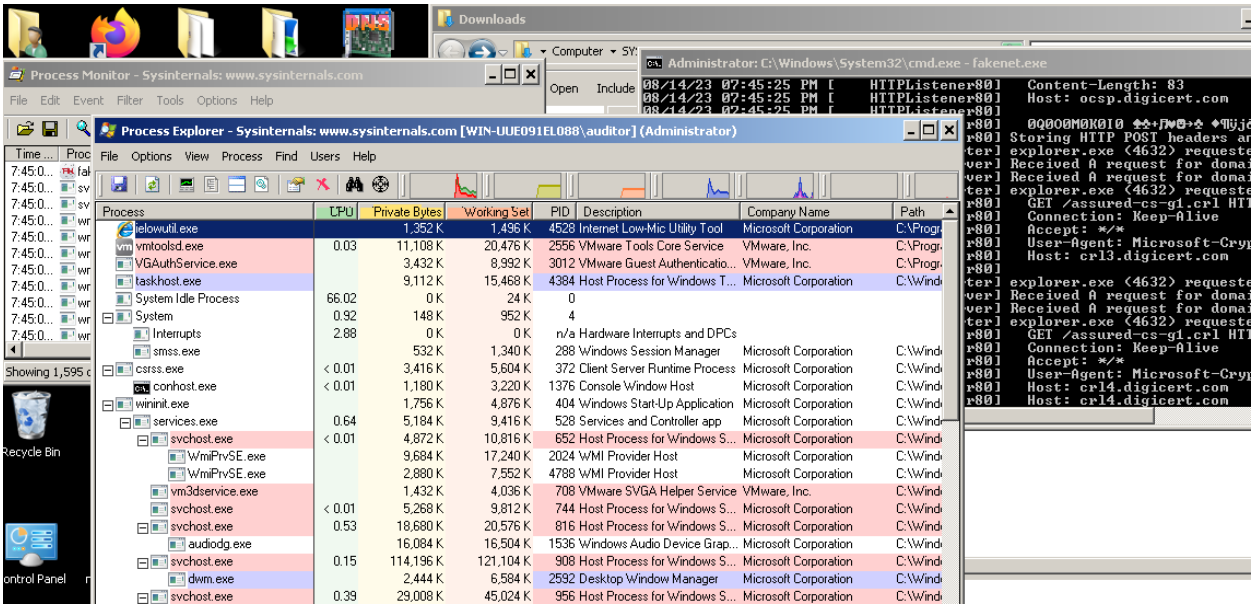
Ideally with observations and evidence above it hides all the main components mentioned by its prefix.

From the evidence of the registry of net wire documents that the malware related to ADVANCED remote access trojan which manipulates by entering to the system by capturing its data , record keyboard strokes and create fake http cookies by talking to internet. (bytecode77, 2022)

According to the reference and the functioning and behavior of the system the rootkit analyzed it matches its functioning of the system according to the reference the solution for the rootkit is to run uninstall.exe for the above GitHub repo might remove above behaviors of the system



Process explorer: used process explorer



During the analysis, the process the services related to the executable file was mentioned yet the process of the executable names was not shown or either hidden

Mitigated solutions

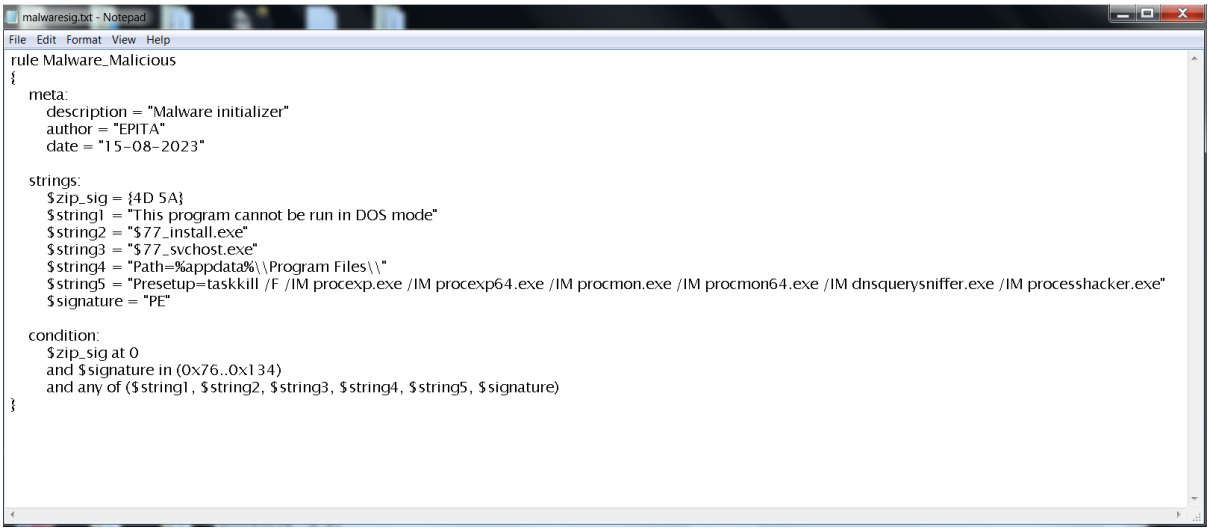
According to the report application is slightly complicated since its natural target and object of behavior is to hide the each and every function under each and every directory, services and also registries.

yet the rootkit had previous history of certain same behavior by running the malware so mainly we should mitigate the system by thoroughly on the static analysis by knowing all the functioning of the malware then better to run to understand of the actions of the system.

Further after the dynamic analysis the cleaning of the system and identification was done by providing a Yara rule.

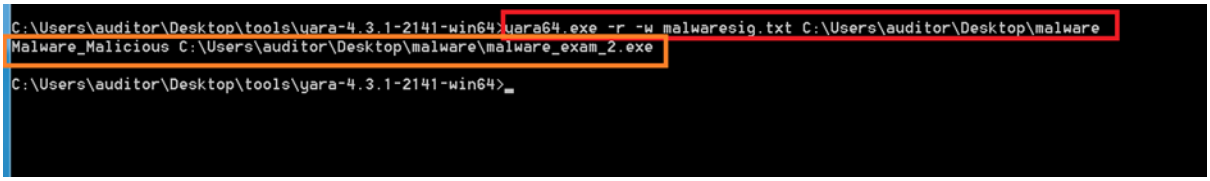
YARA rule system cleanup

Yara rule :



```
rule Malware_Malicious
{
    meta:
        description = "Malware initializer"
        author = "EPITA"
        date = "15-08-2023"

    strings:
        $zip_sig = {4D 5A}
        $string1 = "This program cannot be run in DOS mode"
        $string2 = "$77_install.exe"
        $string3 = "$77_svchost.exe"
        $string4 = "Path=%appdata%\\Program Files\\"
        $string5 = "Presetup=taskkill /F /IM procexp.exe /IM procexp64.exe /IM procmon.exe /IM procmon64.exe /IM dnsquerysniffer.exe /IM processhacker.exe"
        $signature = "PE"

    condition:
        $zip_sig at 0
        and $signature in (0x76..0x134)
        and any of ($string1, $string2, $string3, $string4, $string5, $signature)
}
```

Yara result without showing the detected strings:



```
C:\Users\auditor\Desktop\tools\yara-4.3.1-2141-win64>yara64.exe -r -w malwaresig.txt C:\Users\auditor\Desktop\malware
Malware_Malicious C:\Users\auditor\Desktop\malware\malware_exam_2.exe

C:\Users\auditor\Desktop\tools\yara-4.3.1-2141-win64>
```

Yara result showing the detected strings:

```
C:\Users\auditor\Desktop\tools\yara-4.3.1-2141-win64>yara64.exe -r -w -s malwaresig.txt C:\Users\auditor\Desktop\malware
Malware_Malicious C:\Users\auditor\Desktop\malware\malware_exam_2.exe
0x0:$zip_sig: 4D 5A
0x4e:$string1: This program cannot be run in DOS mode
0x450a2:$string2: $77_install.exe
0x719a0:$string2: $77_install.exe
0xb14bb:$string2: $77_install.exe
0x450d3:$string3: $77_svchost.exe
0x4526a:$string3: $77_svchost.exe
0xb147f:$string3: $77_svchost.exe
0x45064:$string4: Path=%appdata%\Program Files\
0x450e5:$string5: Presetup=taskkill /F /IM procexp.exe /IM procexp64.exe /IM procmon.exe /IM procmon64.exe /IM dnsquerysniffer.exe /IM processhacker.exe
0x118:$signature: PE
0x1d658:$signature: PE
0x1dbe3:$signature: PE
0x23875:$signature: PE
0x26ae1:$signature: PE
0x30e1d:$signature: PE
0x32efa:$signature: PE
0x32fa5:$signature: PE
0x4576e:$signature: PE
0x490db:$signature: PE
0x59d86:$signature: PE
0x6f324:$signature: PE
0x9751e:$signature: PE
0xa3b31:$signature: PE
0xa5815:$signature: PE

C:\Users\auditor\Desktop\tools\yara-4.3.1-2141-win64>^P
```

Yara rule:

```
rule Malware_Malicious
{
   meta:
      description = "Malware initializer"
      author = "Abdallah,Shiron, Inaam"
      date = "15-08-2023"

   strings:
      $zip_sig = {4D 5A}
      $string1 = "This program cannot be run in DOS mode"
      $string2 = "$77_install.exe"
      $string3 = "$77_svchost.exe"
      $string4 = "Path=%appdata%\\Program Files\\"
      $string5 = "Presetup=taskkill /F /IM procexp.exe /IM procexp64.exe /IM procmon.exe /IM procmon64.exe /IM dnsquerysniffer.exe /IM processhacker.exe"
      $signature = "PE"
```

```
    condition:
        $zip_sig at 0
        and $signature in (0x76..0x134)
        and any of ($string1, $string2, $string3, $string4, $string5, $signature)
}
```

Demonstration:

1. Strings Section:

- $zip_sig = {4D 5A}: Searches for the hexadecimal sequence "4D 5A" at the beginning of the malware file (PE header).
- $string1: Searches for the specific string "This program cannot be run in DOS mode" which was shown in the malware file.
- $string2 and $string3: Look for the execution files: "$77_install.exe" and "$77_svchost.exe".
- $string4: Searches for the string "Path=%appdata%\\Program Files\\" which could indicate installation in the user's AppData directory.
- $string5: Searches for a specific string containing a list of processes to be killed (potential malicious activity).
- $signature: Represents the string "PE", commonly found in Portable Executable files.

2. Condition Section:

- $zip_sig at 0: Requires the "4D 5A" signature to be at the file's beginning (indicative of a PE file).
- $signature in (0x76..0x134): Checks for the "PE" signature within a specific range (PE header location).
- any of ($string1, $string2, $string3, $string4, $string5, $signature): A match occurs if any of these strings/signatures are found in the file.

This YARA rule aims to identify potential malicious files based on various indicators present in the given malware code. It checks for known signatures, strings, and sequences that could suggest malicious behavior or characteristics commonly associated with malware. If any of these indicators are found in a file, it could be flagged as suspicious and containing malware.