# Malware Analysis

Final Report

Shannon Dsouza
12-12-2020

# Index

# Synthesis

Malware analysis is the identification of the actions of a malware using static and dynamic analysis. Additionally, by dumping the memory of an infected machine and analysing it using memory forensics tools, the actions of the processes are analysed.

Static analysis tools such as hex editors, detect it easy, and PE-bear are used to analyse the type of the file and the DLLs it imports to guess the actions the malware might perform. The hash of the malware is used to identify if the malware is a known sample.

Dynamic analysis tools such as process monitor and process hacker are used to identify what the malware does when executed. Process monitor records all the operations performed so they can be analysed and process hacker would reveal the name of the created process and any of its child processes.

# Malware Analysis Process

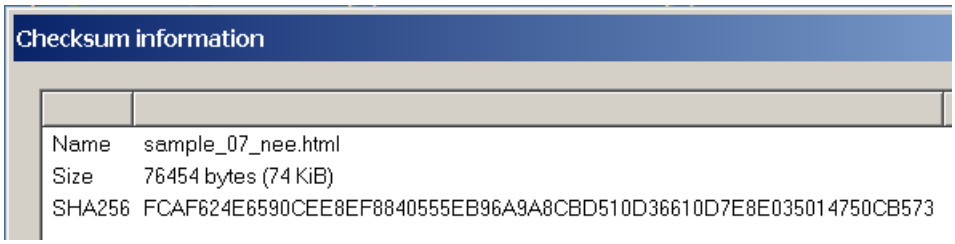
## Binary data manipulation

Description:

The static analysis of the malware uses tools such as a hex editor, Detect It Easy, and the virus total database to identify the malware, its entropy and its type.

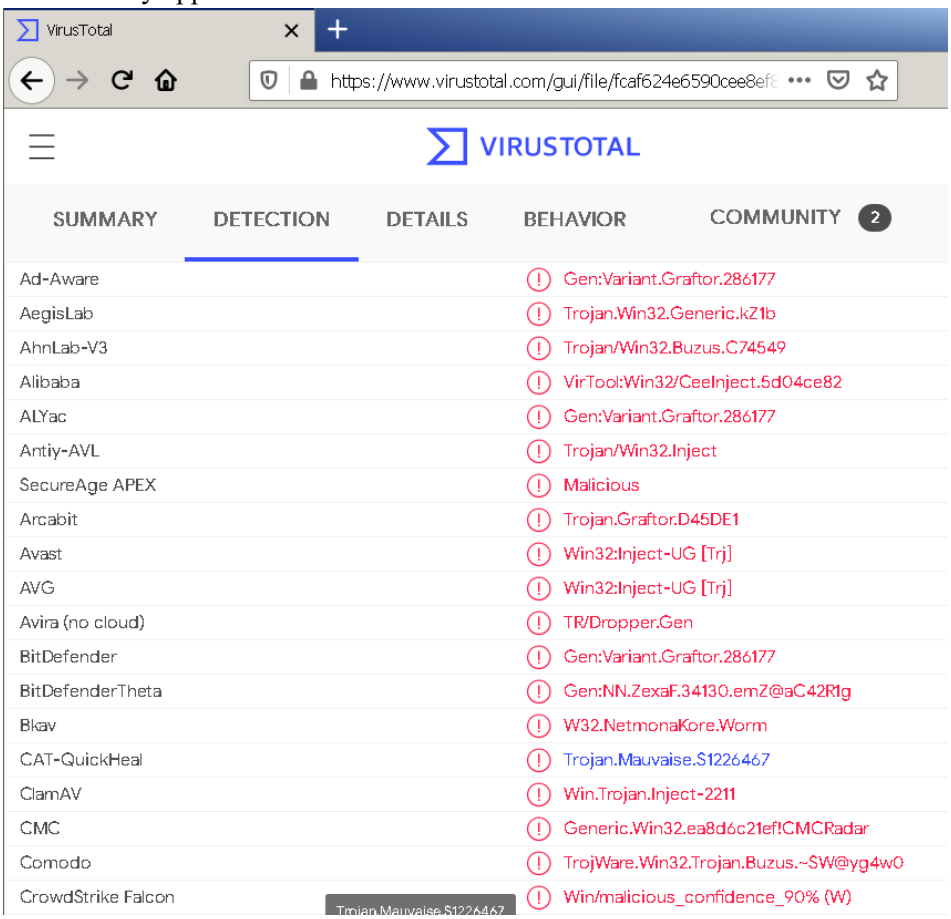
Process:

a) The SHA256 hash of the malware sample is 'FCAF624E6590CEE8EF8840555EB96A9A8CBD510D36610D7E8E035014750CB573'




SHA256 is the ideal hash function to use to compare against a database

b) Using Virus Total, the malware is identified by multiple engines as a 'Graftor'. Searching for graftor malwares shows that it is adware that alters the behaviour of the user's browser and installs unnecessary applications.




Malware repeatedly identified as 'Graftor'

Cisco Talos Intelligence Group -

blog.talosintelligence.com/2017/09/graftor-but-i-never-asked-for-this...

## Overview

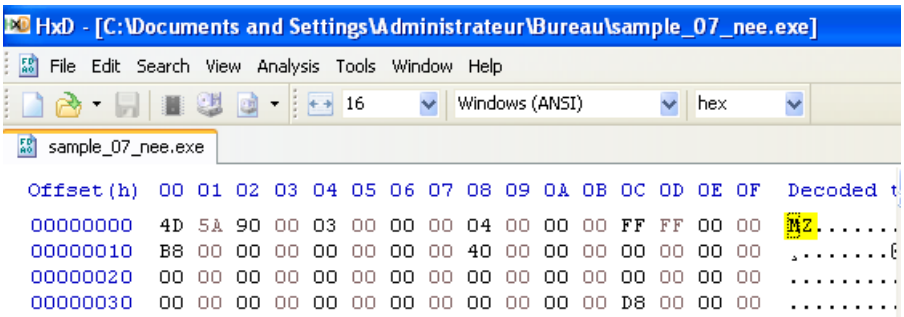
Free software often downloaded from large freeware distribution sites is a boon for the internet, providing users with functionality that otherwise they would not be able to use. Often users, happy that they are getting something free, fail to pay attention to the hints in the licence agreement that they are receiving additional software services bundled with the freeware they desire.

Graftor aka LoadMoney adware dropper is a potentially unwanted program often installed as part of freeware software installers. We wanted to investigate the effects this software has on a user's system. According to the analysis performed in our sandbox, Graftor and the associated affiliate files it downloads perform the following functions:

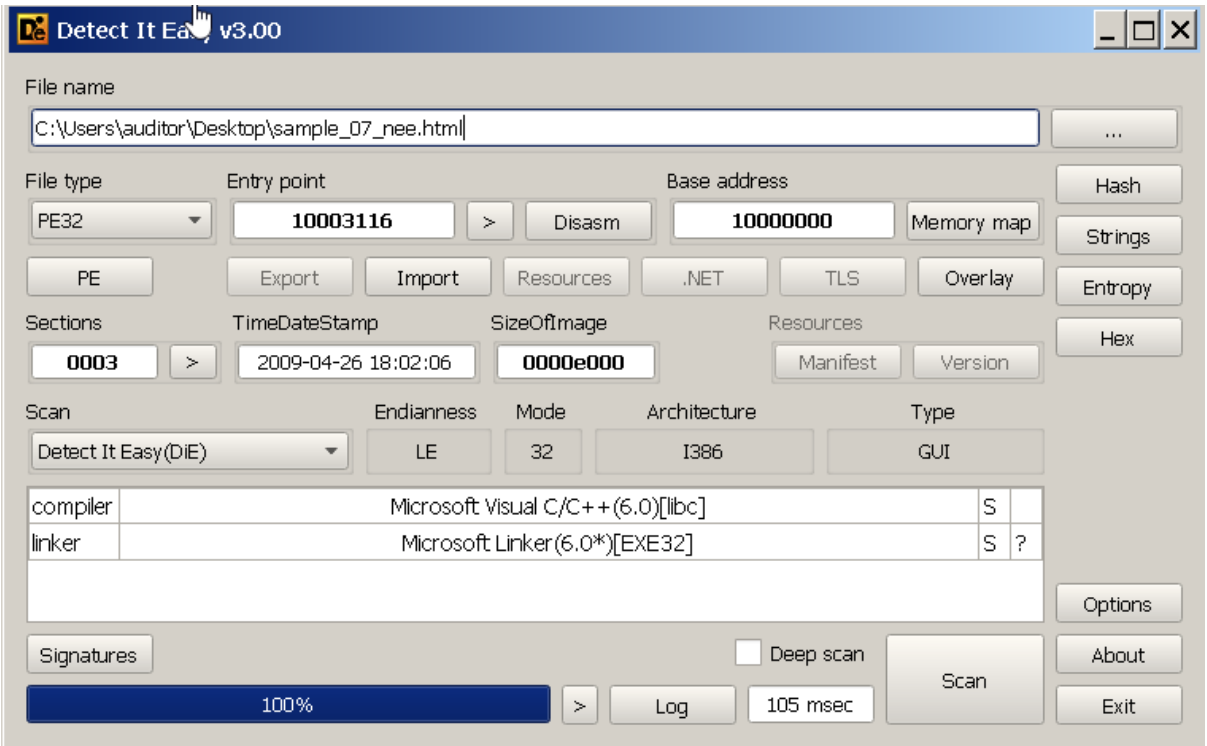
- Hijacks the user's browser and injects advertising banners
- Installs other potentially unwanted applications from partners like mail.ru
- It does not ask the user, it just silently installs these programs
- Random web page text is turned into links
- Adds Desktop and Browser Quick Launch links
- User's homepage is changed
- User's search provider is changed
- Partner adware is executed and it social engineers the user to install further software
- Checks for installed AV software
- Checks for sandbox environments
- Anti-Analysis protection
- Unnecessary API calls to overflow sandbox environments
- Creates/Modifies system certificates

The actions Graftor performs on the compromised machine

c) Using a hex editor[1], the magic bytes of the program are revealed to be 'MZ'. This signifies that the file is an executable. Additionally, using Detect It Easy[2], the file is identified as a PE file - native executable.

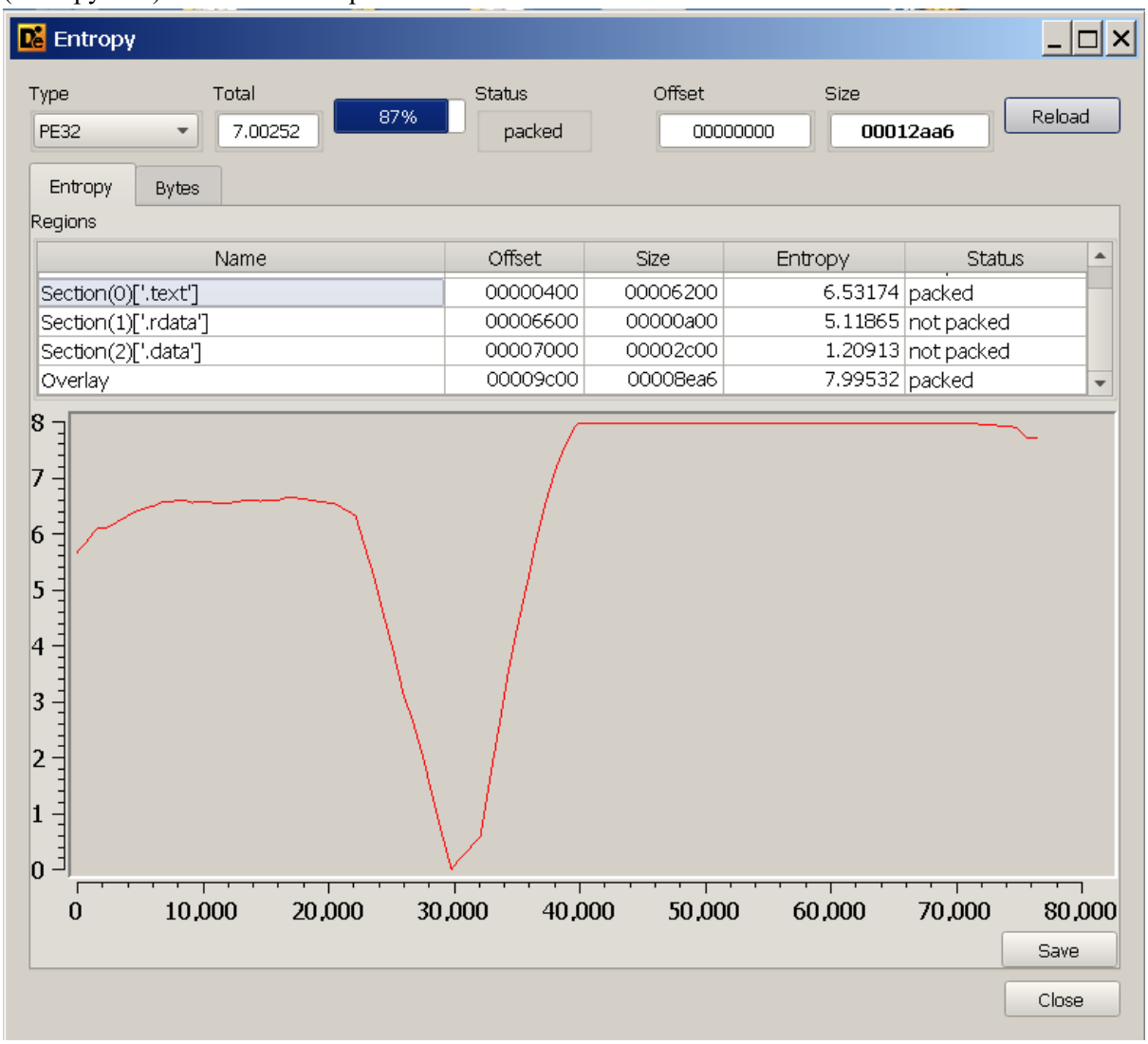



The magic bytes of the malware



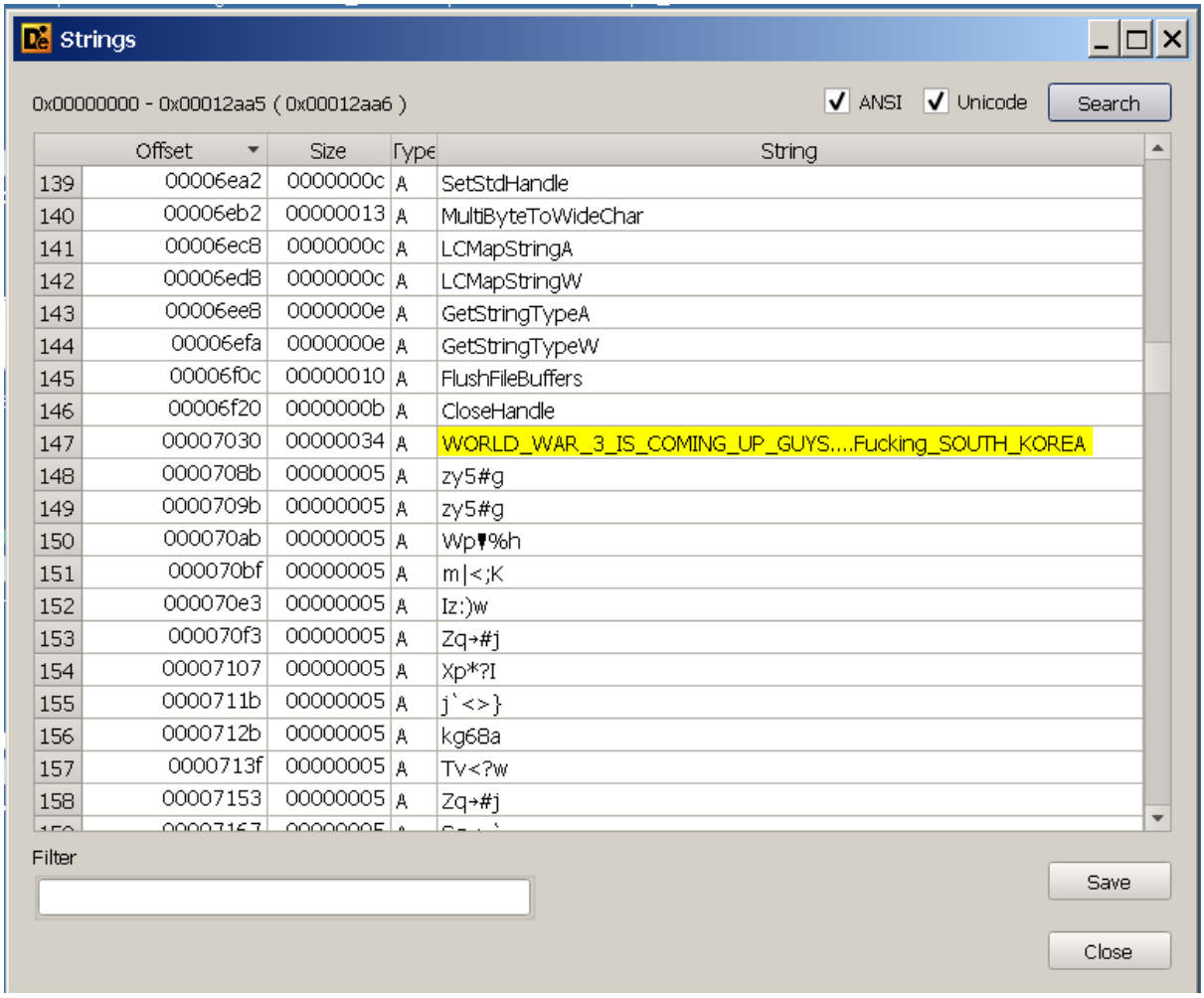

PE file – native executable

d) Detect It Easy also reveals the entropy of the file. The ‘text’ section (Entropy=6.53) is packed and the ‘overlay’ (Entropy=7.99) is packed. The ‘rdata’ (Entropy=5.11) and ‘data’ (Entropy=1.2) sections are not packed.




Entropy distribution across the file

e) Analysing the strings using the sysInternals strings programs, a single unique text string is identified.




| | Offset | Size | Type | String |
|---|---|---|---|---|
| 139 | 00006ea2 | 0000000c | A | SetStdHandle |
| 140 | 00006eb2 | 00000013 | A | MultiByteToWideChar |
| 141 | 00006ec8 | 0000000c | A | LCMapStringA |
| 142 | 00006ed8 | 0000000c | A | LCMapStringW |
| 143 | 00006ee8 | 0000000e | A | GetStringTypeA |
| 144 | 00006efa | 0000000e | A | GetStringTypeW |
| 145 | 00006f0c | 00000010 | A | FlushFileBuffers |
| 146 | 00006f20 | 0000000b | A | CloseHandle |
| 147 | 00007030 | 00000034 | A | WORLD_WAR_3_IS_COMING_UP_GUYS....Fucking_SOUTH_KOREA |
| 148 | 0000708b | 00000005 | A | zy5#g |
| 149 | 0000709b | 00000005 | A | zy5#g |
| 150 | 000070ab | 00000005 | A | Wp▼%h |
| 151 | 000070bf | 00000005 | A | m\|<;K |
| 152 | 000070e3 | 00000005 | A | Iz:)w |
| 153 | 000070f3 | 00000005 | A | Zq→#j |
| 154 | 00007107 | 00000005 | A | Xp*?I |
| 155 | 0000711b | 00000005 | A | j`<>} |
| 156 | 0000712b | 00000005 | A | kg68a |
| 157 | 0000713f | 00000005 | A | Tv<?w |
| 158 | 00007153 | 00000005 | A | Zq→#j |

The identified unique text string


Reference:

[1] https://mh-nexus.de/en/hxd/

[2] https://github.com/horsicq/Detect-It-Easy

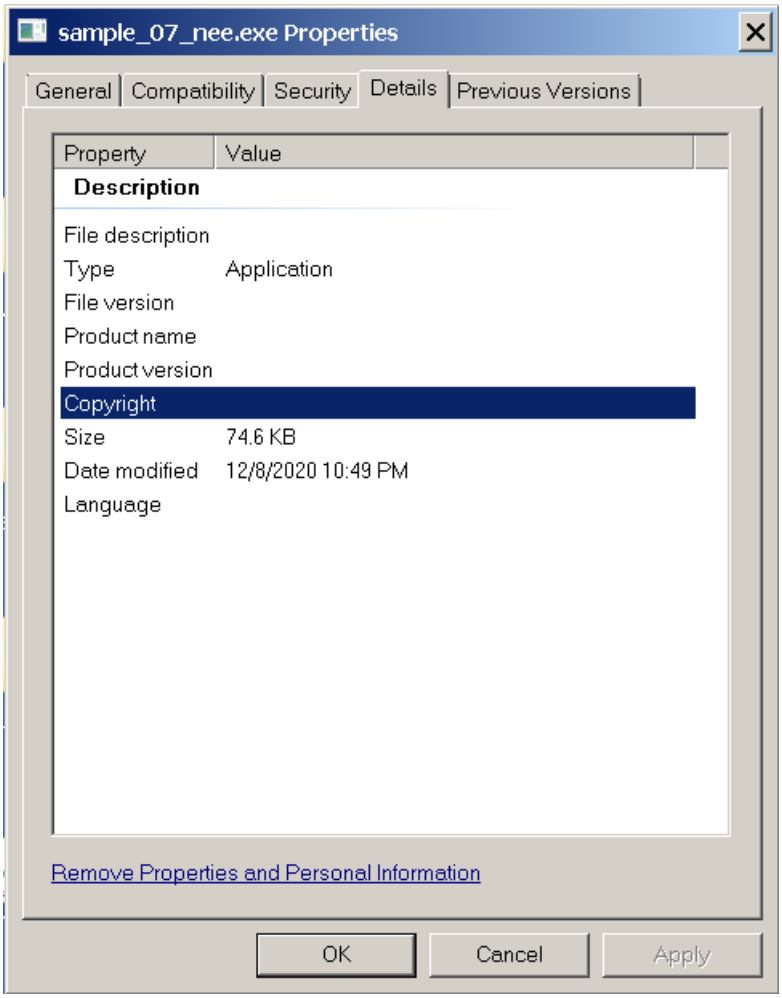
# PE file format analysis

Description:

The file format analysis attempts to discover as much information as possible about the file such as if it is signed, whether it is native code, the type of interface, information about the sections, and the imported and exported DLLs.

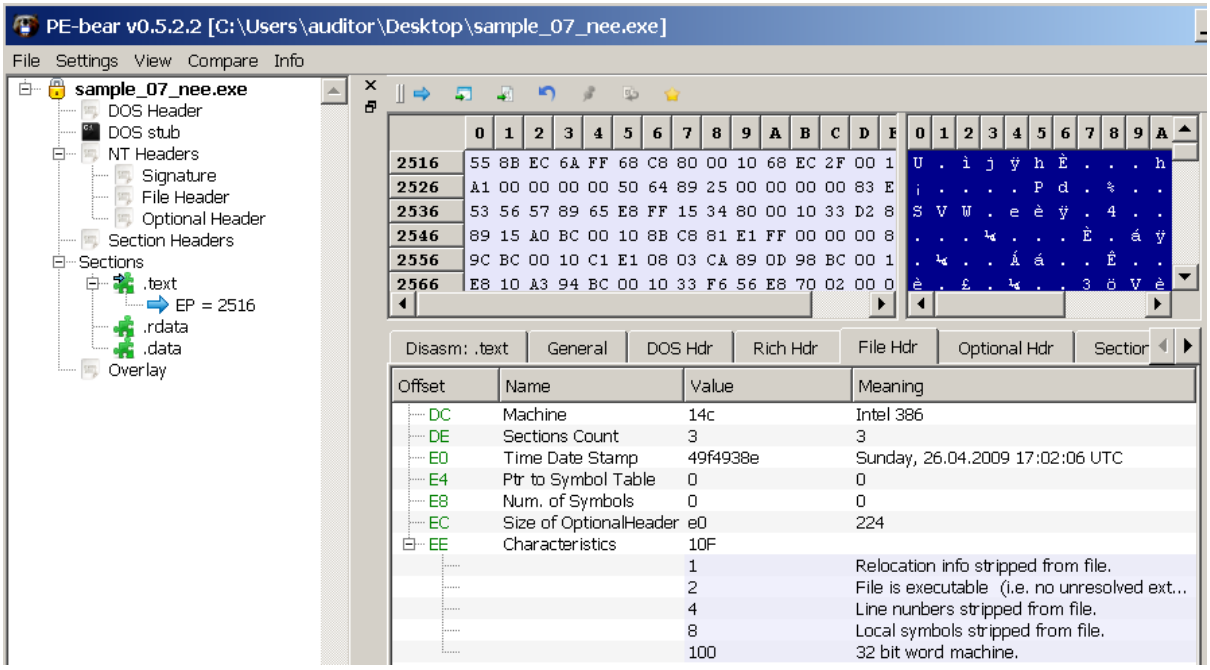
Process:

a) The missing 'Digital Signatures' tab in the properties of the file shows that the executable is not signed. The 'Details' tab reveals that all the metadata of the file has been stripped.



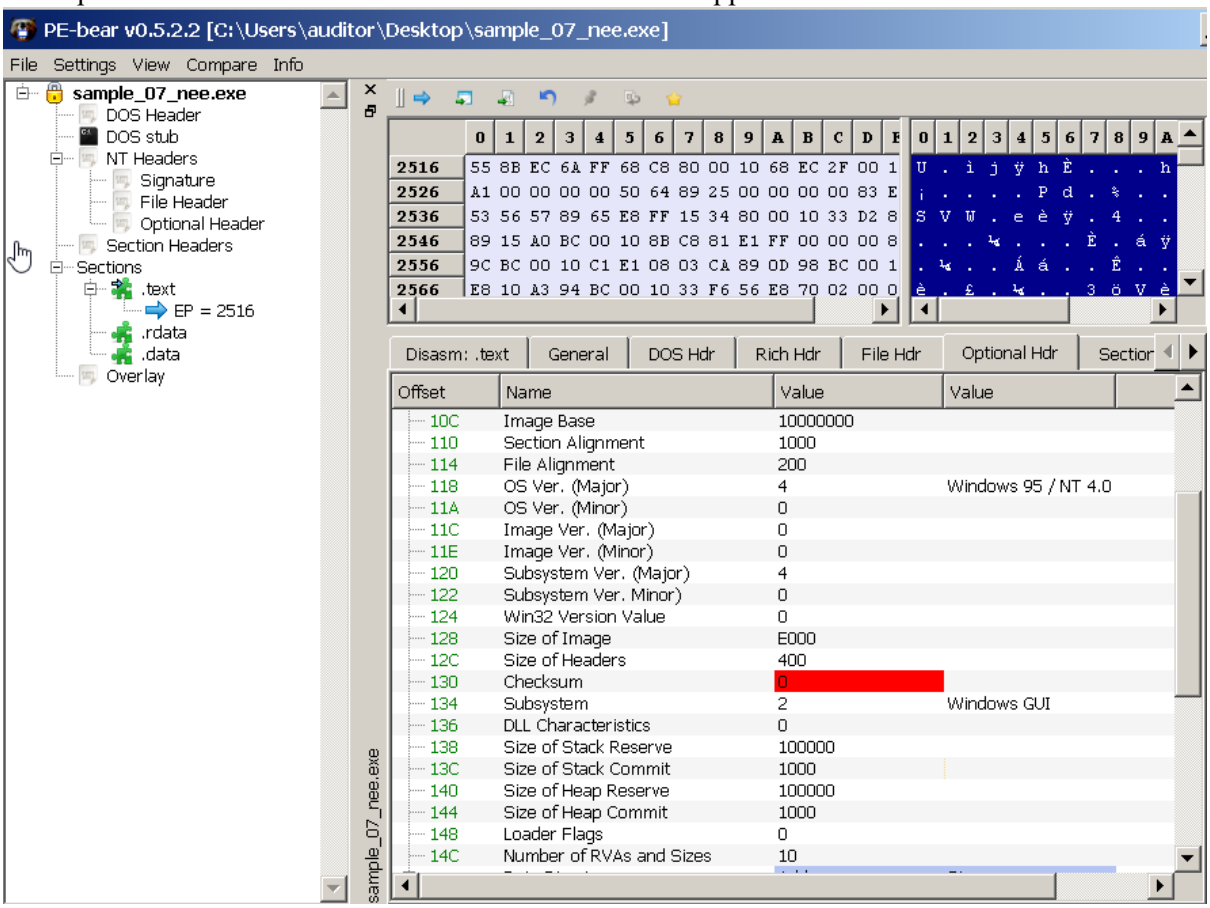

No metadata is present

b) Analysing the executable in PE-bear[3] by hasherezade reveals that it was compiled on 26/04/2009 for a 32-bit intel x86 machine. The file is executable and native code.



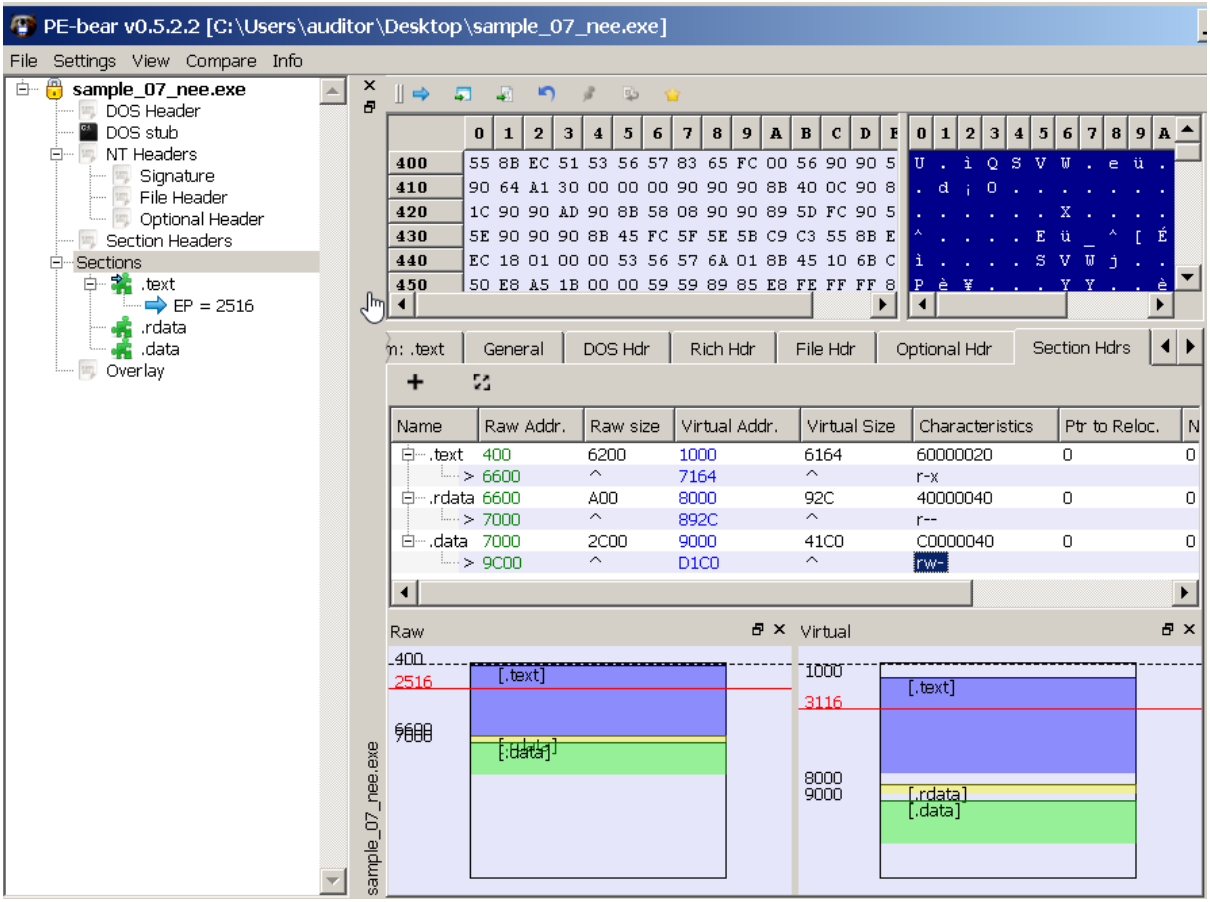

The File Header reveals the compilation date, the file type and the intended architecture

c) The Optional Header tab reveals that the malware is a GUI application.



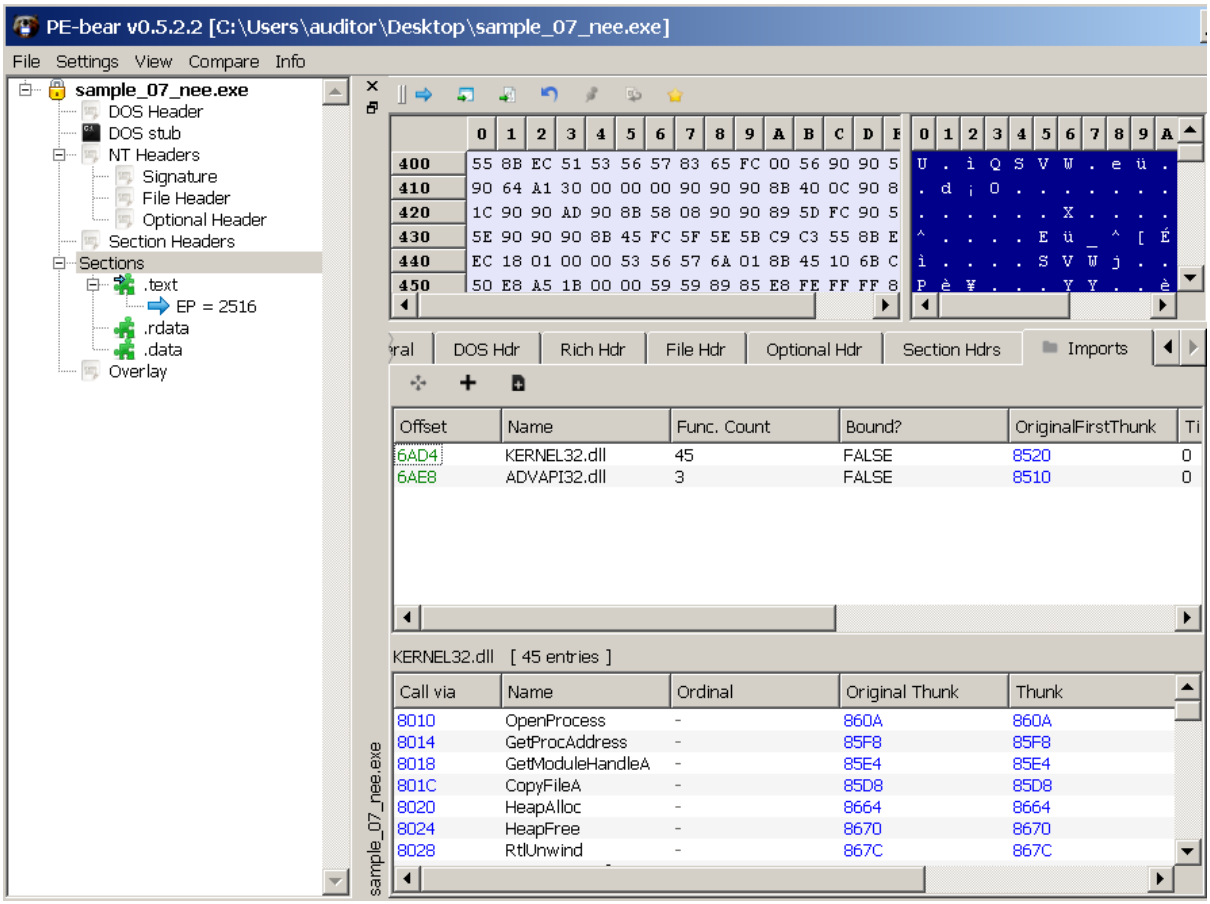

The malware is a GUI app

d) The section header reveals the raw and virtual size of each section, a slight decrease in the virtual size is expected and that is what occurs for the text and rdata sections. However, the data section nearly doubles in virtual size when compared to the raw size. This could mean that the program decompresses the malicious code into the data section. The permissions for each section are valid and not suspicious. The entry points are in the text section as it should be, in the raw state the EP=2516 and in the virtual state the EP=3116.




Information about the sections

e) The Imports tab presents the imported DLLs: KERNEL32.dll and ADVAPI32.dll. The missing Exports tab implies that no DLL is exported. The KERNEL32 DLL is used to manipulate files, such as editing, copying or creating new files, among other file operations. Therefore, this importing of this DLL is suspicious. The ADVAPI32 DLL is used to manipulate the registry, the functions present here are creating a registry key, querying a registry key and deleting a registry key. This is also suspicious.



The DLLs imported by the executable


Reference:

[3] https://github.com/hasherezade/pe-bear-releases

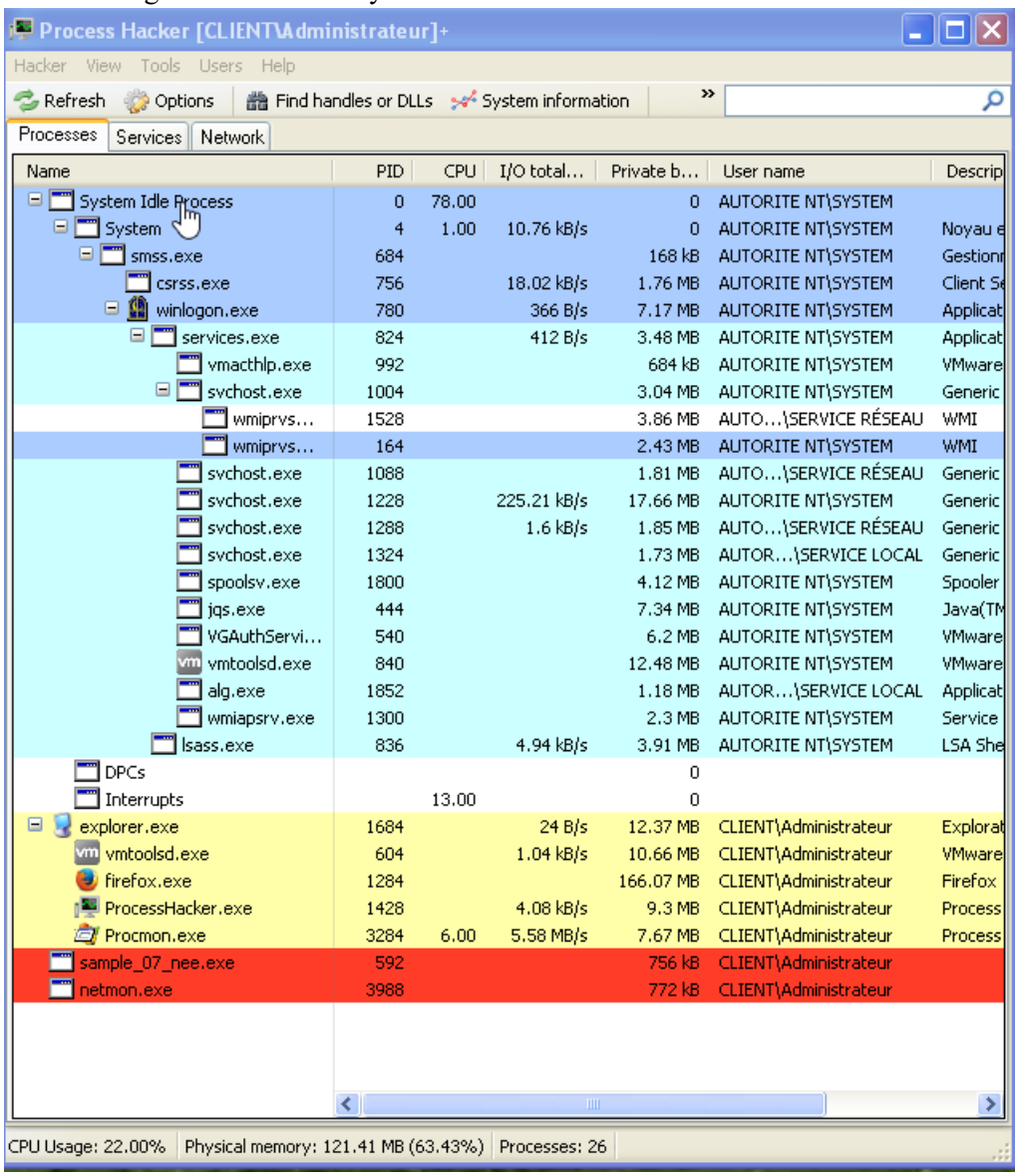
# Dynamic analysis

## Description:

The dynamic analysis is carried out by recording the actions performed by processes while it executes. Process monitor[4] from the sysInternals suite and Process hacker[5] are used to do this analysis. The files created by the malware as well as how it maintains persistence can be identifies using this analysis.

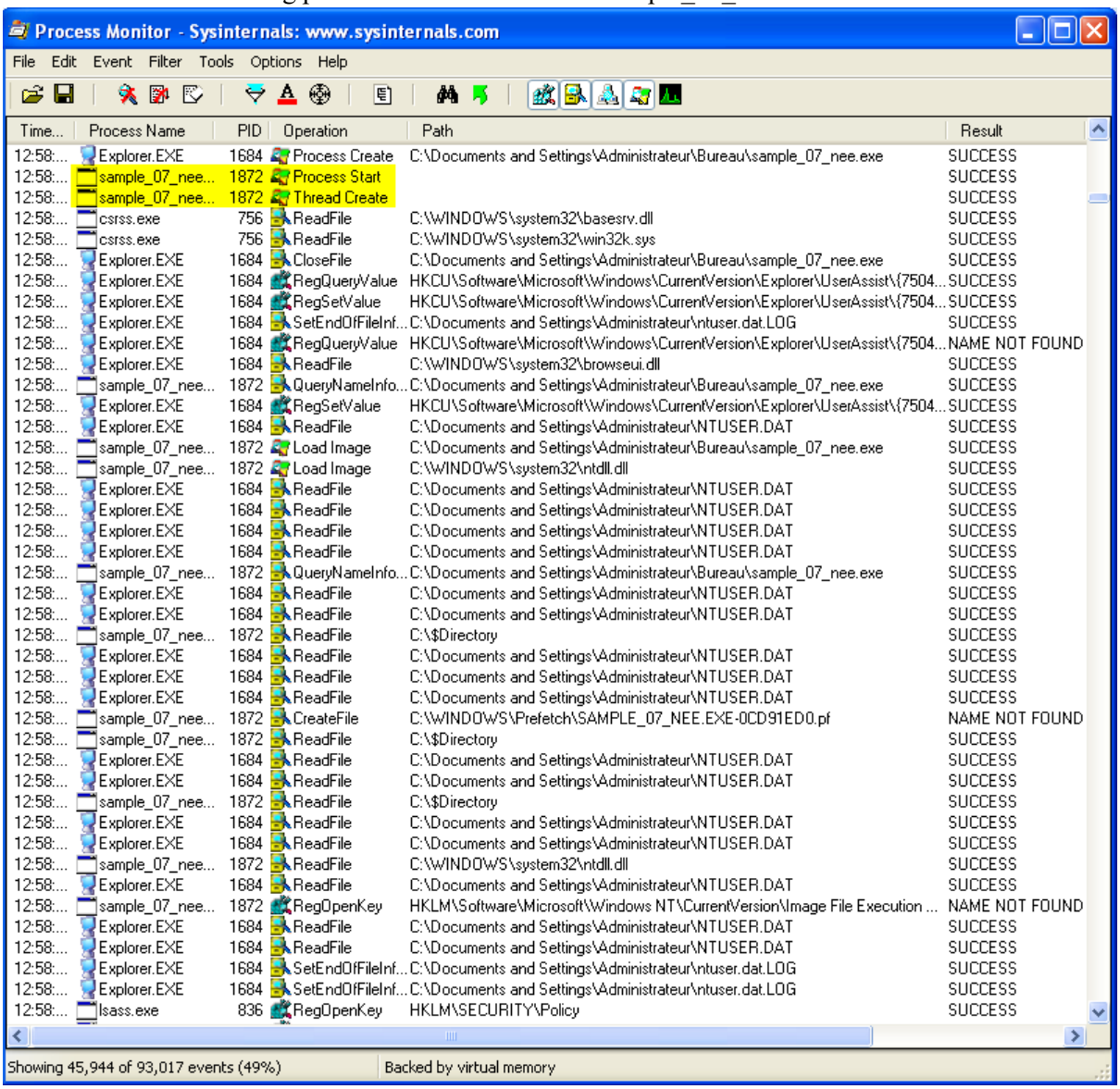
## Process:

a) To revert to a clean state of the sandbox, a snapshot of the system is saved before the malware is executed. Then begin recording the actions performed by the malware using process monitor from the sysInternals suite and view the processes that are created when the malware is executed using Process Hacker by Wen Nia Liu and Steven G.




The processes created when the malware is executed are the executable 'sample_07_nee' itself and a new process called 'netmon'

b) The recorded actions using process monitor reveal that sample_07_nee



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

| Time... | Process Name | PID | Operation | Path | Result |
|---|---|---|---|---|---|
| 12:58:... | Explorer.EXE | 1684 | Process Create | C:\Documents and Settings\Administrateur\Bureau\sample_07_nee.exe | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | Process Start | | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | Thread Create | | SUCCESS |
| 12:58:... | csrss.exe | 756 | ReadFile | C:\WINDOWS\system32\basesrv.dll | SUCCESS |
| 12:58:... | csrss.exe | 756 | ReadFile | C:\WINDOWS\system32\win32k.sys | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | CloseFile | C:\Documents and Settings\Administrateur\Bureau\sample_07_nee.exe | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | RegQueryValue | HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{7504... | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | RegSetValue | HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{7504... | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | SetEndOfFileInf... | C:\Documents and Settings\Administrateur\ntuser.dat.LOG | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | RegQueryValue | HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{7504... | NAME NOT FOUND |
| 12:58:... | Explorer.EXE | 1684 | ReadFile | C:\WINDOWS\system32\browseui.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | QueryNameInfo... | C:\Documents and Settings\Administrateur\Bureau\sample_07_nee.exe | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | RegSetValue | HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{7504... | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | ReadFile | C:\Documents and Settings\Administrateur\NTUSER.DAT | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | Load Image | C:\Documents and Settings\Administrateur\Bureau\sample_07_nee.exe | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | Load Image | C:\WINDOWS\system32\ntdll.dll | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | ReadFile | C:\Documents and Settings\Administrateur\NTUSER.DAT | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | ReadFile | C:\Documents and Settings\Administrateur\NTUSER.DAT | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | ReadFile | C:\Documents and Settings\Administrateur\NTUSER.DAT | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | ReadFile | C:\Documents and Settings\Administrateur\NTUSER.DAT | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | QueryNameInfo... | C:\Documents and Settings\Administrateur\Bureau\sample_07_nee.exe | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | ReadFile | C:\Documents and Settings\Administrateur\NTUSER.DAT | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | ReadFile | C:\Documents and Settings\Administrateur\NTUSER.DAT | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | ReadFile | C:\$Directory | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | ReadFile | C:\Documents and Settings\Administrateur\NTUSER.DAT | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | ReadFile | C:\Documents and Settings\Administrateur\NTUSER.DAT | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | ReadFile | C:\Documents and Settings\Administrateur\NTUSER.DAT | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | CreateFile | C:\WINDOWS\Prefetch\SAMPLE_07_NEE.EXE-0CD91ED0.pf | NAME NOT FOUND |
| 12:58:... | sample_07_nee... | 1872 | ReadFile | C:\$Directory | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | ReadFile | C:\Documents and Settings\Administrateur\NTUSER.DAT | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | ReadFile | C:\Documents and Settings\Administrateur\NTUSER.DAT | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | ReadFile | C:\$Directory | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | ReadFile | C:\Documents and Settings\Administrateur\NTUSER.DAT | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | ReadFile | C:\Documents and Settings\Administrateur\NTUSER.DAT | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | ReadFile | C:\WINDOWS\system32\ntdll.dll | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | ReadFile | C:\Documents and Settings\Administrateur\NTUSER.DAT | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegOpenKey | HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution ... | NAME NOT FOUND |
| 12:58:... | Explorer.EXE | 1684 | ReadFile | C:\Documents and Settings\Administrateur\NTUSER.DAT | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | ReadFile | C:\Documents and Settings\Administrateur\NTUSER.DAT | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | SetEndOfFileInf... | C:\Documents and Settings\Administrateur\ntuser.dat.LOG | SUCCESS |
| 12:58:... | Explorer.EXE | 1684 | SetEndOfFileInf... | C:\Documents and Settings\Administrateur\ntuser.dat.LOG | SUCCESS |
| 12:58:... | lsass.exe | 836 | RegOpenKey | HKLM\SECURITY\Policy | SUCCESS |

Showing 45,944 of 93,017 events (49%) | Backed by virtual memory

The starting of the process and creation of the thread

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

| Time... | Process Name | PID | Operation | Path | Result |
|---|---|---|---|---|---|
| 12:58:... | sample_07_nee... | 1872 | RegOpenKey | HKLM\System\CurrentControlSet\Control\Terminal Server | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegQueryValue | HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegCloseKey | HKLM\System\CurrentControlSet\Control\Terminal Server | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | ReadFile | C:\WINDOWS\system32\secur32.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | ReadFile | C:\WINDOWS\system32\secur32.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | ReadFile | C:\WINDOWS\system32\rpcrt4.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | ReadFile | C:\WINDOWS\system32\advapi32.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegOpenKey | HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution ... | NAME NOT FOUND |
| 12:58:... | sample_07_nee... | 1872 | ReadFile | C:\WINDOWS\system32\rpcrt4.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegOpenKey | HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution ... | NAME NOT FOUND |
| 12:58:... | sample_07_nee... | 1872 | RegOpenKey | HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution ... | NAME NOT FOUND |
| 12:58:... | sample_07_nee... | 1872 | RegOpenKey | HKLM\System\CurrentControlSet\Control\Terminal Server | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegQueryValue | HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegQueryValue | HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegCloseKey | HKLM\System\CurrentControlSet\Control\Terminal Server | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegOpenKey | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegQueryValue | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTr... | NAME NOT FOUND |
| 12:58:... | sample_07_nee... | 1872 | RegCloseKey | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegOpenKey | HKLM | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegOpenKey | HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics | NAME NOT FOUND |
| 12:58:... | sample_07_nee... | 1872 | RegOpenKey | HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution ... | NAME NOT FOUND |
| 12:58:... | sample_07_nee... | 1872 | RegOpenKey | HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution ... | NAME NOT FOUND |
| 12:58:... | sample_07_nee... | 1872 | ReadFile | C:\Documents and Settings\Administrateur\Bureau\sample_07_nee.exe | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | ReadFile | C:\Documents and Settings\Administrateur\Bureau\sample_07_nee.exe | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | ReadFile | C:\WINDOWS\system32\ctype.nls | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | ReadFile | C:\WINDOWS\system32\sortkey.nls | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | ReadFile | C:\WINDOWS\system32\kernel32.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegOpenKey | HKCU | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegOpenKey | HKCU\Control Panel\Sound | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | ReadFile | C:\Documents and Settings\Administrateur\NTUSER.DAT | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegQueryValue | HKCU\Control Panel\Sound\Beep | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegQueryValue | HKCU\Control Panel\Sound\Beep | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegCloseKey | HKCU\Control Panel\Sound | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegOpenKey | HKLM\System\CurrentControlSet\Control\Session Manager | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegQueryValue | HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode | NAME NOT FOUND |
| 12:58:... | sample_07_nee... | 1872 | RegCloseKey | HKLM\System\CurrentControlSet\Control\Session Manager | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | RegCloseKey | <INVALID NAME> | INVALID HANDLE |
| 12:58:... | sample_07_nee... | 1872 | CreateFile | C:\Documents and Settings\Administrateur\Bureau\sample_07_nee.exe | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | QueryStandardI... | C:\Documents and Settings\Administrateur\Bureau\sample_07_nee.exe | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | ReadFile | C:\Documents and Settings\Administrateur\Bureau\sample_07_nee.exe | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | ReadFile | C:\Documents and Settings\Administrateur\Bureau\sample_07_nee.exe | SUCCESS |
| 12:58:... | sample_07_nee... | 1872 | CloseFile | C:\Documents and Settings\Administrateur\Bureau\sample_07_nee.exe | SUCCESS |

Showing 45,944 of 93,017 events (49%) Backed by virtual memory

The malware tests whether it has access to create keys in several paths

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

| Time... | Process Name | PID | Operation | Path | Result |
|---|---|---|---|---|---|
| 12:58:... | sample_07_nee... | 592 | QueryOpen | C:\Documents and Settings\Administrateur\Bureau\WS2HELP.dll | NAME NOT FOUND |
| 12:58:... | sample_07_nee... | 592 | QueryOpen | C:\WINDOWS\system32\ws2help.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | CreateFile | C:\WINDOWS\system32\ws2help.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | CreateFileMapp... | C:\WINDOWS\system32\ws2help.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | CreateFileMapp... | C:\WINDOWS\system32\ws2help.dll | SUCCESS |
| 12:58:... | svchost.exe | 1228 | CloseFile | C:\WINDOWS\system32\ctype.nls | SUCCESS |
| 12:58:... | svchost.exe | 1228 | QueryOpen | C:\WINDOWS\system32\kernel32.dll | SUCCESS |
| 12:58:... | svchost.exe | 1228 | CreateFile | C:\WINDOWS\system32\kernel32.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | CloseFile | C:\WINDOWS\system32\ws2help.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | Load Image | C:\WINDOWS\system32\ws2help.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | ReadFile | C:\WINDOWS\system32\wsock32.dll | SUCCESS |
| 12:58:... | svchost.exe | 1228 | QueryFileIntern... | C:\WINDOWS\system32\kernel32.dll | SUCCESS |
| 12:58:... | svchost.exe | 1228 | CloseFile | C:\WINDOWS\system32\kernel32.dll | SUCCESS |
| 12:58:... | svchost.exe | 1228 | QueryOpen | C:\WINDOWS\system32\locale.nls | SUCCESS |
| 12:58:... | svchost.exe | 1228 | CreateFile | C:\WINDOWS\system32\locale.nls | SUCCESS |
| 12:58:... | svchost.exe | 1228 | QueryFileIntern... | C:\WINDOWS\system32\locale.nls | SUCCESS |
| 12:58:... | svchost.exe | 1228 | CloseFile | C:\WINDOWS\system32\locale.nls | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | Load Image | C:\WINDOWS\system32\mpr.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | ReadFile | C:\WINDOWS\system32\mpr.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | ReadFile | C:\WINDOWS\system32\mpr.dll | SUCCESS |
| 12:58:... | svchost.exe | 1228 | QueryOpen | C:\WINDOWS\system32\ntdll.dll | SUCCESS |
| 12:58:... | svchost.exe | 1228 | CreateFile | C:\WINDOWS\system32\ntdll.dll | SUCCESS |
| 12:58:... | svchost.exe | 1228 | QueryFileIntern... | C:\WINDOWS\system32\ntdll.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | ReadFile | C:\WINDOWS\system32\shlwapi.dll | SUCCESS |
| 12:58:... | svchost.exe | 1228 | CloseFile | C:\WINDOWS\system32\ntdll.dll | SUCCESS |
| 12:58:... | svchost.exe | 1228 | QueryOpen | C:\WINDOWS\system32\rpcrt4.dll | SUCCESS |
| 12:58:... | svchost.exe | 1228 | CreateFile | C:\WINDOWS\system32\rpcrt4.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | Load Image | C:\WINDOWS\system32\comctl32.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | ReadFile | C:\WINDOWS\system32\comctl32.dll | SUCCESS |
| 12:58:... | svchost.exe | 1228 | QueryFileIntern... | C:\WINDOWS\system32\rpcrt4.dll | SUCCESS |
| 12:58:... | svchost.exe | 1228 | CloseFile | C:\WINDOWS\system32\rpcrt4.dll | SUCCESS |
| 12:58:... | svchost.exe | 1228 | QueryOpen | C:\WINDOWS\system32\secur32.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | ReadFile | C:\WINDOWS\system32\comctl32.dll | SUCCESS |
| 12:58:... | svchost.exe | 1228 | CreateFile | C:\WINDOWS\system32\secur32.dll | SUCCESS |
| 12:58:... | svchost.exe | 1228 | QueryFileIntern... | C:\WINDOWS\system32\secur32.dll | SUCCESS |
| 12:58:... | svchost.exe | 1228 | CloseFile | C:\WINDOWS\system32\secur32.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | CreateFile | C:\Documents and Settings\Administrateur\Bureau\sample_07_nee.exe | SUCCESS |
| 12:58:... | svchost.exe | 1228 | QueryOpen | C:\WINDOWS\system32\sortkey.nls | SUCCESS |
| 12:58:... | svchost.exe | 1228 | CreateFile | C:\WINDOWS\system32\sortkey.nls | SUCCESS |
| 12:58:... | svchost.exe | 1228 | QueryFileIntern... | C:\WINDOWS\system32\sortkey.nls | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | ReadFile | C:\Documents and Settings\Administrateur\Bureau\sample_07_nee.exe | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | CloseFile | C:\Documents and Settings\Administrateur\Bureau\sample_07_nee.exe | SUCCESS |

Showing 45,944 of 93,017 events (49%) Backed by virtual memory

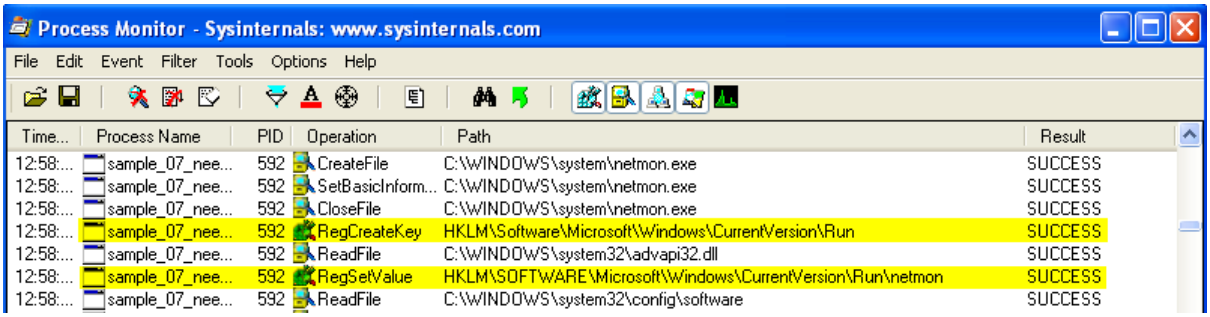
The malware accesses several DLLs not identified using the static analysis phase

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

| Time... | Process Name | PID | Operation | Path | Result |
|---|---|---|---|---|---|
| 12:58:... | sample_07_nee... | 592 | QueryEaInform... | C:\Documents and Settings\Administrateur\Bureau\sample_07_nee.exe | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | CreateFile | C:\WINDOWS\system\netmon.exe | SUCCESS |
| 12:58:... | winlogon.exe | 780 | ReadFile | C:\WINDOWS\system32\sfc_os.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | QueryAttributel... | C:\WINDOWS\system\netmon.exe | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | QueryBasicInfor... | C:\WINDOWS\system\netmon.exe | SUCCESS |

The malware creates an executable called netmon

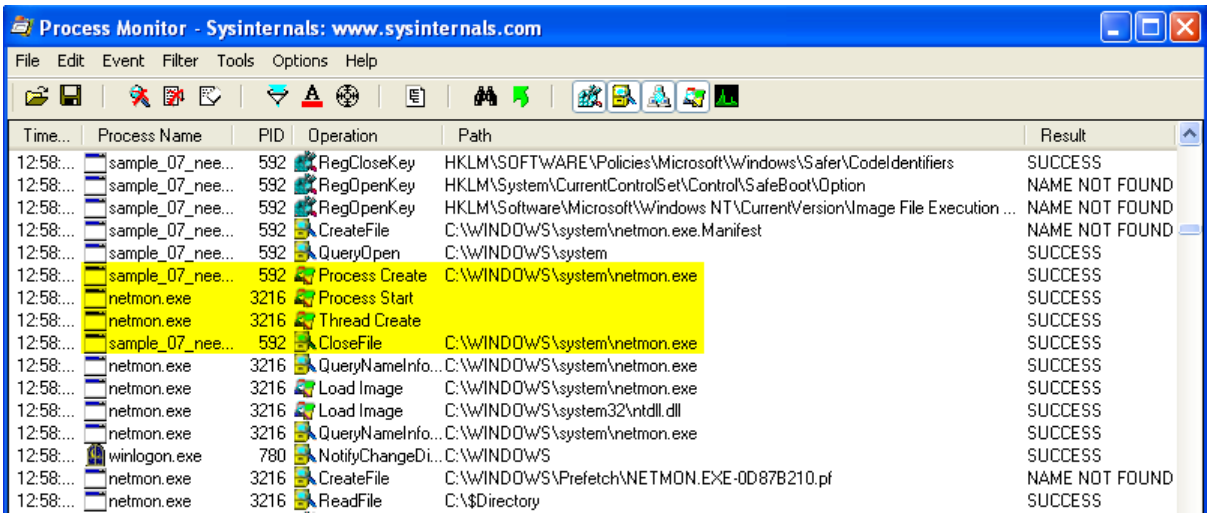


Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

| Time... | Process Name | PID | Operation | Path | Result |
|---|---|---|---|---|---|
| 12:58:... | sample_07_nee... | 592 | CreateFile | C:\WINDOWS\system\netmon.exe | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | SetBasicInform... | C:\WINDOWS\system\netmon.exe | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | CloseFile | C:\WINDOWS\system\netmon.exe | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | RegCreateKey | HKLM\Software\Microsoft\Windows\CurrentVersion\Run | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | ReadFile | C:\WINDOWS\system32\advapi32.dll | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | RegSetValue | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\netmon | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | ReadFile | C:\WINDOWS\system32\config\software | SUCCESS |

The malware creates a persistence mechanism by adding a registry key for netmon in 'SOFTWARE\Microsoft\Windows\CurrentVersion\Run'



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

| Time... | Process Name | PID | Operation | Path | Result |
|---|---|---|---|---|---|
| 12:58:... | sample_07_nee... | 592 | RegCloseKey | HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | RegOpenKey | HKLM\System\CurrentControlSet\Control\SafeBoot\Option | NAME NOT FOUND |
| 12:58:... | sample_07_nee... | 592 | RegOpenKey | HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution ... | NAME NOT FOUND |
| 12:58:... | sample_07_nee... | 592 | CreateFile | C:\WINDOWS\system\netmon.exe.Manifest | NAME NOT FOUND |
| 12:58:... | sample_07_nee... | 592 | QueryOpen | C:\WINDOWS\system | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | Process Create | C:\WINDOWS\system\netmon.exe | SUCCESS |
| 12:58:... | netmon.exe | 3216 | Process Start | | SUCCESS |
| 12:58:... | netmon.exe | 3216 | Thread Create | | SUCCESS |
| 12:58:... | sample_07_nee... | 592 | CloseFile | C:\WINDOWS\system\netmon.exe | SUCCESS |
| 12:58:... | netmon.exe | 3216 | QueryNameInfo... | C:\WINDOWS\system\netmon.exe | SUCCESS |
| 12:58:... | netmon.exe | 3216 | Load Image | C:\WINDOWS\system\netmon.exe | SUCCESS |
| 12:58:... | netmon.exe | 3216 | Load Image | C:\WINDOWS\system32\ntdll.dll | SUCCESS |
| 12:58:... | netmon.exe | 3216 | QueryNameInfo... | C:\WINDOWS\system\netmon.exe | SUCCESS |
| 12:58:... | winlogon.exe | 780 | NotifyChangeDi... | C:\WINDOWS | SUCCESS |
| 12:58:... | netmon.exe | 3216 | CreateFile | C:\WINDOWS\Prefetch\NETMON.EXE-0D87B210.pf | NAME NOT FOUND |
| 12:58:... | netmon.exe | 3216 | ReadFile | C:\$Directory | SUCCESS |

Sample_07_nee creates a process for netmon and then netmon starts the process and creates a thread for itself. Finally, sample_07_nee deletes itself

Reference:


[4] https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite

[5] https://processhacker.sourceforge.io/

# Memory analysis

Description:

By dumping the memory of the infected machine, we can analyse it using a tool such as volatility [6] from the volatility foundation. We can identify processes created by the malware, how it manages persistence, the network connections it makes, and its mutexes. We can also identify the memory pages that seem malicious and dump them. The malicious process itself is also dumped and analysed.

Process:

a) Using volatility and running the psscan command, a process named netmon with a PID=3988 is discovered. Its parent ID is 3216 which is not present in the results of psscan. From our earlier analysis we know the netmon process was created by the sample_07_nee process, so the PID=3216 must be of that process.

```
Command Prompt
Offset(P)          Name                 PID   PPID PDB        Time created
------------------ ---------------- ------ ------ ---------- ------------------------------
---------------
0x000000000005e020 svchost.exe        1228    824 0x09e40120 2020-12-09 18:39:01 UTC+0000
0x0000000000e11a10 regedit.exe        3048   3284 0x09e40300 2020-12-12 13:21:29 UTC+0000
1:34 UTC+0000
0x0000000000e11da0 explorer.exe       1684   1652 0x09e401c0 2020-12-09 18:39:02 UTC+0000
0x0000000001088b68 services.exe        824    780 0x09e40080 2020-12-09 18:39:01 UTC+0000
0x00000000010c4da0 smss.exe            684      4 0x09e40020 2020-12-09 18:39:00 UTC+0000
0x000000000110d1e0 svchost.exe        1004    824 0x09e400e0 2020-12-09 18:39:01 UTC+0000
0x000000000113dda0 vmacthlp.exe        992    824 0x09e400c0 2020-12-09 18:39:01 UTC+0000
0x000000000121dda0 System                4      0 0x006e6000
0x0000000001de7cb8 vmtoolsd.exe        604   1684 0x09e40180 2020-12-09 18:39:14 UTC+0000
0x0000000001f72458 die.exe            3672   2872 0x09e40220 2020-12-10 21:35:06 UTC+0000
6:12 UTC+0000
0x000000000290dda0 Procmon.exe        3284   1684 0x09e40280 2020-12-12 11:56:31 UTC+0000
0x00000000051da020 lsass.exe           836    780 0x09e400a0 2020-12-09 18:39:01 UTC+0000
0x00000000051fe118 csrss.exe           756    684 0x09e40040 2020-12-09 18:39:01 UTC+0000
0x0000000005231020 firefox.exe        1284   1684 0x09e401a0 2020-12-09 18:39:57 UTC+0000
0x0000000005284698 svchost.exe        1088    824 0x09e40100 2020-12-09 18:39:01 UTC+0000
0x00000000052b59b8 alg.exe            1852    824 0x09e40240 2020-12-09 18:39:13 UTC+0000
0x000000000533fda0 svchost.exe        1288    824 0x09e40140 2020-12-09 18:39:01 UTC+0000
0x0000000005361020 ProcessHacker.e    1428   1684 0x09e40360 2020-12-12 11:47:28 UTC+0000
0x000000000568b700 jqs.exe             444    824 0x09e40260 2020-12-09 18:39:12 UTC+0000
0x0000000005b7f700 regedit.exe        2580   3284 0x09e40320 2020-12-12 13:26:23 UTC+0000
6:25 UTC+0000
0x0000000005d83da0 svchost.exe        1324    824 0x09e40160 2020-12-09 18:39:01 UTC+0000
0x0000000005dc5da0 winlogon.exe        780    684 0x09e40060 2020-12-09 18:39:01 UTC+0000
0x0000000006454ba8 DumpIt.exe         3164   1684 0x09e403c0 2020-12-12 13:58:06 UTC+0000
0x00000000065193c0 spoolsv.exe        1800    824 0x09e401e0 2020-12-09 18:39:02 UTC+0000
0x0000000006639d60 firefox.exe        3452   1284 0x09e40340 2020-12-11 22:55:41 UTC+0000
9:17 UTC+0000
0x00000000006790bb8 wmiapsrv.exe      1300    824 0x09e40200 2020-12-09 18:39:14 UTC+0000
0x0000000006e40568 wmiprvse.exe       1528   1004 0x09e402a0 2020-12-09 18:39:12 UTC+0000
0x000000000741da98 VGAuthService.e     540    824 0x09e402c0 2020-12-09 18:39:12 UTC+0000
0x00000000075b01d0 vmtoolsd.exe        840    824 0x09e402e0 2020-12-09 18:39:12 UTC+0000
0x000000000afc6340 netmon.exe         3988   3216 0x09e403a0 2020-12-12 11:58:59 UTC+0000
```

The suspicious process ‘netmon’

b) Running the connscan command reveals several connections made by netmon.

Command Prompt

| Offset(P) | Local Address | Remote Address | Pid |
|---|---|---|---|
| 0x0009d620 | 192.168.221.132:2032 | 192.168.106.124:445 | 3988 |
| 0x004ad410 | 192.168.221.132:2200 | 192.168.42.191:445 | 3988 |
| 0x00857608 | 92.4.178.241:53246 | 0.0.0.0:28814 | 0 |
| 0x00857a88 | 92.4.178.241:2815 | 60.0.128.32:24730 | 11984896 |
| 0x00857cc8 | 8.0.0.0:21504 | 255.0.0.0:19968 | 5439558 |
| 0x00a2ae68 | 192.168.221.132:445 | 192.168.221.132:1513 | 4 |
| 0x00a80588 | 192.168.221.132:2120 | 192.168.3.15:445 | 3988 |
| 0x00d4a760 | 127.0.0.1:1038 | 127.0.0.1:1039 | 1284 |
| 0x00d7fb48 | 192.168.221.132:2137 | 192.168.231.192:445 | 3988 |
| 0x00e8d008 | 192.168.63.128:3098 | 192.168.63.128:445 | 3988 |
| 0x00e8d980 | 192.168.63.128:3099 | 192.168.63.128:445 | 4 |
| 0x00f53490 | 192.168.221.132:2070 | 192.168.6.135:445 | 3988 |
| 0x00f539d0 | 192.168.221.132:2119 | 192.168.213.100:445 | 3988 |
| 0x010f4e38 | 192.168.221.132:445 | 192.168.221.132:3275 | 4 |
| 0x0113be68 | 192.168.221.132:2124 | 192.168.114.226:445 | 3988 |
| 0x016b65d0 | 192.168.221.132:2141 | 192.168.189.143:445 | 3988 |
| 0x01a1ea10 | 1.0.0.0:51454 | 104.0.0.0:45098 | 1024 |
| 0x01b1ba80 | 192.168.221.132:2195 | 192.168.176.192:445 | 3988 |
| 0x01b1bc30 | 192.168.221.132:2544 | 192.168.134.240:445 | 3988 |
| 0x01d229c0 | 192.168.221.132:3972 | 192.168.116.93:445 | 3988 |
| 0x01e74b50 | 192.168.63.128:445 | 192.168.63.128:3099 | 4 |
| 0x01f379d0 | 192.168.221.132:2151 | 192.168.121.249:445 | 3988 |
| 0x01fd6790 | 192.168.221.132:3921 | 192.168.144.78:445 | 3988 |
| 0x023af5c8 | 192.168.221.132:2084 | 192.168.36.192:445 | 3988 |
| 0x024fa360 | 192.168.221.132:1889 | 192.168.35.70:445 | 0 |
| 0x024fa658 | 192.168.221.132:1949 | 192.168.144.75:445 | 3988 |
| 0x024fa920 | 192.168.221.132:2038 | 192.168.193.2:445 | 3988 |
| 0x025cae68 | 192.168.221.132:2135 | 192.168.45.63:445 | 3988 |
| 0x026e3a00 | 192.168.221.132:2146 | 192.168.45.186:445 | 3988 |
| 0x0283fd98 | 192.168.221.132:2139 | 192.168.22.47:445 | 3988 |
| 0x0284c588 | 192.168.221.132:2148 | 192.168.212.94:445 | 3988 |
| 0x0284ce68 | 192.168.221.132:2122 | 192.168.97.189:445 | 3988 |
| 0x02c8d388 | 192.168.221.132:1979 | 192.168.238.253:445 | 3988 |
| 0x02d099e0 | 192.168.221.132:2156 | 192.168.8.51:445 | 3988 |
| 0x02d6c008 | 192.168.63.128:445 | 192.168.63.128:1749 | 4 |
| 0x02d72978 | 192.168.221.132:1796 | 192.168.129.100:445 | 45350916 |
| 0x0318c328 | 0.112.163.11:0 | 0.0.0.0:0 | 4096 |
| 0x0318c5b0 | 192.168.221.132:2121 | 192.168.190.144:445 | 3988 |
| 0x0318cc28 | 192.168.221.132:2013 | 192.168.66.57:445 | 3988 |
| 0x03221758 | 192.168.63.128:3100 | 192.168.63.128:445 | 3988 |
| 0x03385260 | 253.2.0.0:0 | 67.99.66.99:16 | 0 |
| 0x0346ce68 | 64.0.0.0:50942 | 0.0.0.0:43140 | 4274888320 |
| 0x03643e68 | 192.168.221.132:2126 | 192.168.91.142:445 | 3988 |
| 0x0387b1f0 | 192.168.221.132:1869 | 192.168.145.97:445 | 0 |
| 0x0387b390 | 192.168.221.132:1870 | 192.168.54.89:445 | 0 |
| 0x0387ba58 | 192.168.221.132:1513 | 192.168.221.132:445 | 3988 |
| 0x03c7ae68 | 192.168.63.128:1749 | 192.168.63.128:445 | 3988 |

As all the IPs are private IPs, it isn't directly identifiable as an entity

c) From previous analysis, persistence is obtained by adding a registry key in SOFTWARE\Microsoft\Windows\CurrentVersion\Run. Looking for the same key using volatility shows no results, this implies that the key was not saved in memory.

```
Command Prompt

Virtual    Physical   Name
---------- ---------- ----
0xe16b66b8 0x0b6a66b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe135e960 0x0a5b6960 [no name]
0xe10182f8 0x08deb2f8 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe1008b60 0x0585eb60 [no name]
0xe18fa818 0x08b73818 \Device\HarddiskVolume1\Documents and Settings\Administrateur\Local Settings\Applicat
ion Data\Microsoft\Windows\UsrClass.dat
0xe25a8b60 0x07b1ab60 \Device\HarddiskVolume1\Documents and Settings\Administrateur\NTUSER.DAT
0xe1c97008 0x0a3bc008 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Applicatio
n Data\Microsoft\Windows\UsrClass.dat
0xe1c908d8 0x099798d8 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe1c74520 0x07b7c520 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Applicat
ion Data\Microsoft\Windows\UsrClass.dat
0xe1c6d488 0x04d06488 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe16b6210 0x0b6a6210 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe150f280 0x01ad8280 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe1511b60 0x07509b60 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM

E:\volatility-master>C:\Python27\python vol.py -f malware.raw printkey -o 0xe10182f8 -K "Microsoft\Windows\
CurrentVersion\Run"
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
Legend: (S) = Stable   (V) = Volatile

The requested key could not be found in the hive(s) searched
```

The registry key is not saved on memory

d) The mutexes of the malware can be identified using the handles command on volatility.

```
E:\volatility-master>C:\Python27\python vol.py -f malware.raw handles -p 3988 -t "Mutant" --offset=0x0afc63
40
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
Offset(V)     Pid     Handle     Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0xfee60348   3988       0x5c   0x1f0001 Mutant           LxLXsithwarlordXLxL
0xff340158   3988      0x36c   0x1f0001 Mutant           HGFSMUTEX
```

The netmon process has two mutexes

e) Dumping the process using volatility we can analyse the executable, as the first dump did not have the ImageBase address, a second dump is taken to obtain the executable. We can then analyse the executable using a program like strings.

```
Command Prompt

E:\volatility-master>C:\Python27\python vol.py -f malware.raw procdump -p 3988 -D / --offset=0x000000000
afc6340
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)

*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)

*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0xfeeb5340 0x29a00000 netmon.exe           Error: ImageBaseAddress at 0x29a00000 is unavailable (possibl
y due to paging)
```

First dump unable to obtain the executable

```
Command Prompt

E:\volatility-master>C:\Python27\python vol.py -f newmalware.raw procdump -p 2564 -D / --offset=0x07214820
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0xff1cb820 0x29a00000 netmon.exe           OK: executable.2564.exe
```

The second dump is able to dump the process

711 matches found... - C:\Documents and Settings\Administrateur\Bureau\executable.2564.exe

Find | Find | All | Save As | Min Size 4 | Rescan | save min | Offsets | raw

```
.rdata:29A08B98  ExitProcess
.rdata:29A08BA6  CreateProcessA
.rdata:29A08BB8  SetErrorMode
.rdata:29A08BC8  ReleaseMutex
.rdata:29A08BD8  GetCurrentProcessId
.rdata:29A08BEE  CreateMutexA
.rdata:29A08BFE  GetCurrentThread
.rdata:29A08C12  GetFileAttributesA
.rdata:29A08C28  SetProcessPriorityBoost
.rdata:29A08C42  SetThreadPriority
.rdata:29A08C56  SetPriorityClass
.rdata:29A08C6A  GetEnvironmentVariableA
.rdata:29A08C84  GetShortPathNameA
.rdata:29A08C98  GetTempPathA
.rdata:29A08CA8  LockResource
.rdata:29A08CB8  SizeofResource
.rdata:29A08CCA  LoadResource
.rdata:29A08CDA  FindResourceA
.rdata:29A08CE8  KERNEL32.dll
.rdata:29A08CF8  GetForegroundWindow
.rdata:29A08D0C  USER32.dll
.rdata:29A08D1A  OpenSCManagerA
.rdata:29A08D2C  CloseServiceHandle
.rdata:29A08D42  CreateServiceA
.rdata:29A08D54  OpenServiceA
.rdata:29A08D64  StartServiceA
.rdata:29A08D74  QueryServiceStatus
.rdata:29A08D8A  DeleteService
.rdata:29A08D9A  AdjustTokenPrivileges
.rdata:29A08DB2  LookupPrivilegeValueA
.rdata:29A08DCA  OpenProcessToken
.rdata:29A08DDE  RegCloseKey
.rdata:29A08DEC  RegSetValueExA
.rdata:29A08DFE  RegCreateKeyExA
.rdata:29A08E10  RegOpenKeyExA
.rdata:29A08E20  RegDeleteValueA
.rdata:29A08E32  GetUserNameA
.rdata:29A08E40  ADVAPI32.dll
.rdata:29A08E50  ShellExecuteA
.rdata:29A08E60  SHChangeNotify
.rdata:29A08E72  ShellExecuteExA
.rdata:29A08E82  SHELL32.dll
.rdata:29A08E8E  WSOCK32.dll
```

Strings retrieved from the dumped process

f) The malfind command on volatility shows all the memory pages that seem malicious due to suspicious permissions. The processes obtained are csrss.exe and explorer.exe, these processes are dumped and analysed to identify if the malware injected into them. However, no suspicious strings were identified in these pages.

```
Command Prompt
E:\volatility-master>C:\Python27\python vol.py -f malware.raw malfind -D /
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)

*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)

*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
WARNING : volatility.debug    : For best results please install distorm3
Process: csrss.exe Pid: 756 Address: 0x7f6f0000
Vad Tag: Vad  Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x000000007f6f0000  c8 00 00 00 42 01 00 00 ff ee ff ee 08 70 00 00   ....B........p..
0x000000007f6f0010  08 00 00 00 00 fe 00 00 00 00 10 00 00 20 00 00   ................
0x000000007f6f0020  00 02 00 00 00 20 00 00 8d 01 00 00 ff ef fd 7f   ................
0x000000007f6f0030  03 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00   ................



Process: explorer.exe Pid: 1684 Address: 0x2590000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x0000000002590000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x0000000002590010  00 00 59 02 00 00 00 00 00 00 00 00 00 00 00 00   ..Y.............
0x0000000002590020  10 00 59 02 00 00 00 00 00 00 00 00 00 00 00 00   ..Y.............
0x0000000002590030  20 00 59 02 00 00 00 00 00 00 00 00 00 00 00 00   ..Y.............
```

Malfind presents pages it thinks are suspicious

53 matches found... - C:\Documents and Settings\Administrateur\Bureau\process.0xff312118.0x7f6f

Find | Find | All | Save As | Min Size 4 | Rescan | save min | Offs

```
00001FE4  00000409
00002170  C:\WINDOWS
00002190  C:\WINDOWS\system32
000021C0  \BaseNamedObjects
0000221C  Clock.ini
00002264  Software\Microsoft\Clock
000022D4  control.ini
0000230C  Color Schemes
0000233C  Control Panel\Color Schemes
000023B4  Current
000023DC  Control Panel\Current
00002444  Custom Colors
00002474  Control Panel\Custom Colors
000024EC  don't load
00002514  Control Panel\don't load
00002584  drivers.desc
000025B4  Microsoft\Windows NT\CurrentVersion\drivers.desc
00002654  MMCPL
00002674  Control Panel\MMCPL
000026DC  Patterns
00002704  Control Panel\Patterns
00002774  related.desc
000027A4  Microsoft\Windows NT\CurrentVersion\related.desc
00002844  Screen Saver.3DFlowerBox
0000288C  Control Panel\Screen Saver.3DFlowerBox
0000291C  Screen Saver.3DFlyingObj
00002964  Control Panel\Screen Saver.3DFlyingObj
000029F4  Screen Saver.3DMaze
00002A34  Control Panel\Screen Saver.3DMaze
00002AB4  Screen Saver.3DPipes
00002AF4  Control Panel\Screen Saver.3DPipes
00002B7C  Screen Saver.3DText
00002BBC  Control Panel\Screen Saver.3DText
00002C3C  Screen Saver.Bezier
00002C7C  Control Panel\Screen Saver.Bezier
00002CFC  Screen Saver.Marquee
00002D3C  Control Panel\Screen Saver.Marquee
00002DC4  Screen Saver.Mystify
00002E04  Control Panel\Screen Saver.Mystify
00002E8C  Screen Saver.Stars
00002EC4  Control Panel\Screen Saver.Stars
00002F44  Userinstallable.drivers
00002F8C  Microsoft\Windows NT\CurrentVersion\Userinstallable.driver
```

Analysing these pages do not reveal anything suspicious

<u>Reference:</u>

[6] https://github.com/volatilityfoundation/volatility