Questions & Answers for Malware Analysts

Presented By,

Bashetty Arun Kumar

Master of Computer Security

EPITA-2018

Questions for Malware Analysts:

1.what are the characteristics of the sample?

- PEiD,
- CFFExplorer,
- Strings,
- sha256sum,
- md5sum

2- how does the sample survive to reboot?

3- what is the CnC IP/domain name?

4- what are the create/dropped files on disk?

5- what does it do?

6- how to clean the system?

=>After research I found that the given file is netmon.exe.

What is netmon.exe?

1. netmon.exe is a process which is registered mass-mailing worm.

2. Non-system processes like netmon.exe originate from software you installed on your system.

3. Since most applications store data on your hard disk and in your system's registry, it is likely that your computer has suffered fragmentation and accumulated invalid entries which can affect your PC's performance.

4. The netmon.exe is an executable file on your computer's hard drive. This file contains machine code. If you start the software Trojan.W32.MIMAIL on your PC, the commands contained in netmon.exe will be executed on your PC

5. For this purpose, the file is loaded into the main memory (RAM) and runs there as a Trojan.W32.MIMAIL process (also called a task).

Is netmon.exe harmful?

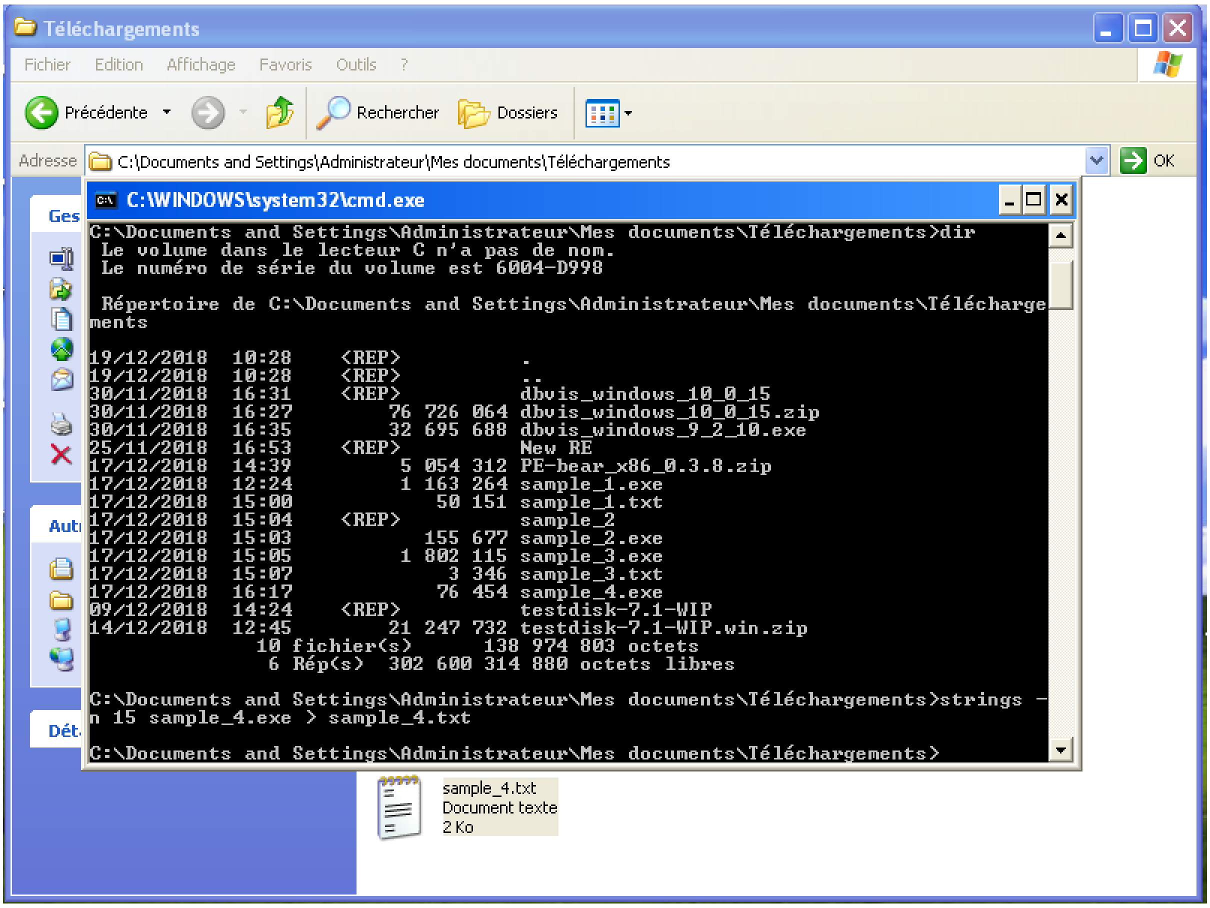
Warning! netmon.exe is considered to be a dangerous process and should be removed. Running issues with this process can increase the risk of malware infection if bugs are present.

Process name: Trojan.W32.MIMAIL

What are the characteristics of the sample?

Strings:

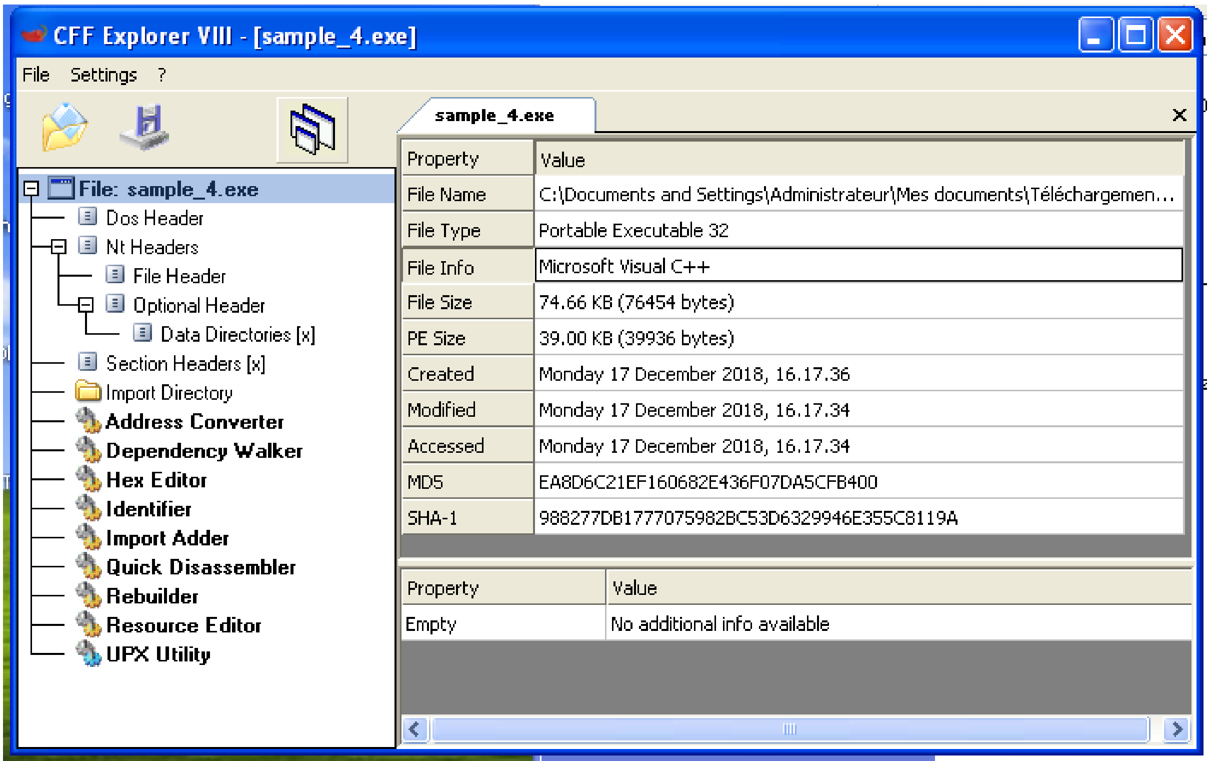
Before converting to strings, you have to download application from http://www.adeleda.com/epita/malwares/exercises/ and change the extension to .exe


Téléchargements
Fichier Edition Affichage Favoris Outils ?
Précédente
Rechercher
Dossiers
Adresse C:\Documents and Settings\Administrateur\Mes documents\Téléchargements
OK
C:\WINDOWS\system32\cmd.exe
sample_4.txt
Document texte
2 Ko

```
C:\Documents and Settings\Administrateur\Mes documents\Téléchargements>dir
 Le volume dans le lecteur C n'a pas de nom.
 Le numéro de série du volume est 6004-D998

 Répertoire de C:\Documents and Settings\Administrateur\Mes documents\Télécharge
ments

19/12/2018  10:28    <REP>          .
19/12/2018  10:28    <REP>          ..
30/11/2018  16:31    <REP>          dbvis_windows_10_0_15
30/11/2018  16:27        76 726 064 dbvis_windows_10_0_15.zip
30/11/2018  16:35        32 695 688 dbvis_windows_9_2_10.exe
25/11/2018  16:53    <REP>          New RE
17/12/2018  14:39         5 054 312 PE-bear_x86_0.3.8.zip
17/12/2018  12:24         1 163 264 sample_1.exe
17/12/2018  15:00            50 151 sample_1.txt
17/12/2018  15:04    <REP>          sample_2
17/12/2018  15:03           155 677 sample_2.exe
17/12/2018  15:05         1 802 115 sample_3.exe
17/12/2018  15:07             3 346 sample_3.txt
17/12/2018  16:17            76 454 sample_4.exe
09/12/2018  14:24    <REP>          testdisk-7.1-WIP
14/12/2018  12:45        21 247 732 testdisk-7.1-WIP.win.zip
              10 fichier(s)      138 974 803 octets
               6 Rép(s)  302 600 314 880 octets libres

C:\Documents and Settings\Administrateur\Mes documents\Téléchargements>strings -
n 15 sample_4.exe > sample_4.txt

C:\Documents and Settings\Administrateur\Mes documents\Téléchargements>
```

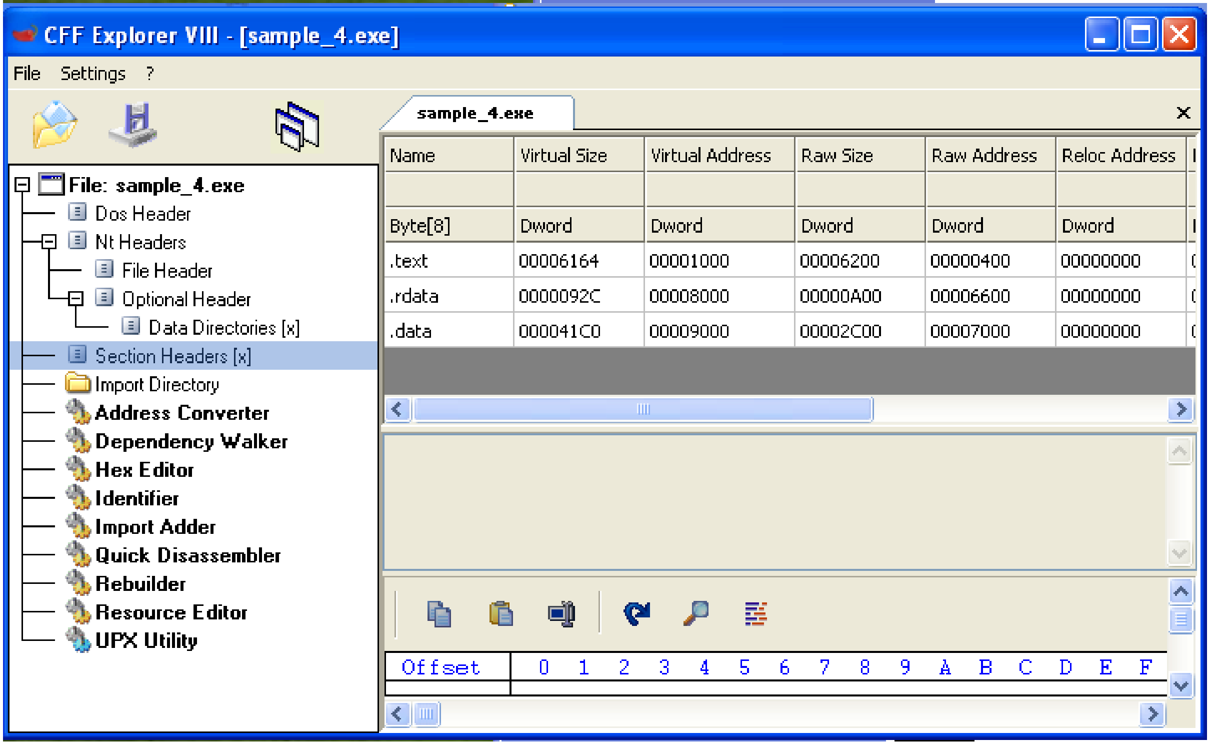
After changing the extension, open the cmd from windows option and give a path, that where you downloaded your file.
After that use strings command and create a new file name and save the strings.

CFF Explorer:



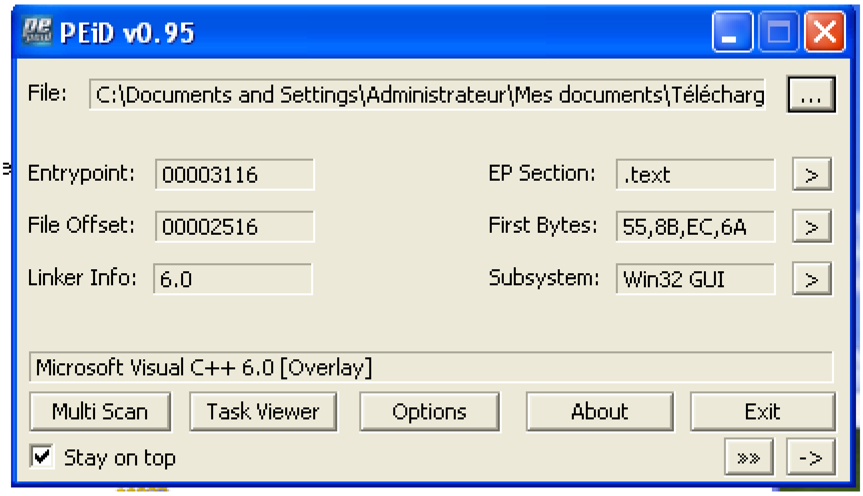
Property	Value
File Name	C:\Documents and Settings\Administrateur\Mes documents\Téléchargemen...
File Type	Portable Executable 32
File Info	Microsoft Visual C++
File Size	74.66 KB (76454 bytes)
PE Size	39.00 KB (39936 bytes)
Created	Monday 17 December 2018, 16.17.36
Modified	Monday 17 December 2018, 16.17.34
Accessed	Monday 17 December 2018, 16.17.34
MD5	EA8D6C21EF160682E436F07DA5CFB400
SHA-1	988277DB1777075982BC53D6329946E355C8119A

Property	Value
Empty	No additional info available



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address
Byte[8]	Dword	Dword	Dword	Dword	Dword
.text	00006164	00001000	00006200	00000400	00000000
.rdata	0000092C	00008000	00000A00	00006600	00000000
.data	000041C0	00009000	00002C00	00007000	00000000

PEiD:



File: C:\Documents and Settings\Administrateur\Mes documents\Télécharg

Entrypoint: 00003116

EP Section: .text

File Offset: 00002516

First Bytes: 55,8B,EC,6A

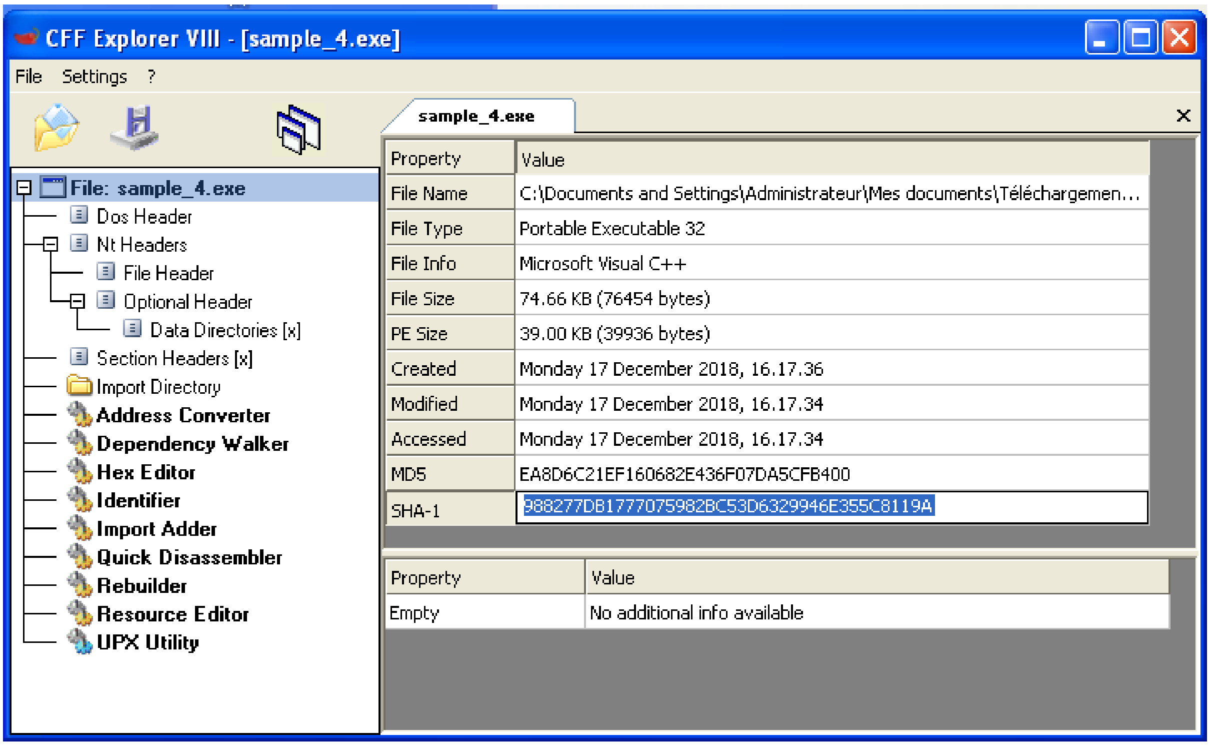
Linker Info: 6.0

Subsystem: Win32 GUI

Microsoft Visual C++ 6.0 [Overlay]

☑ Stay on top

Sha256sum:



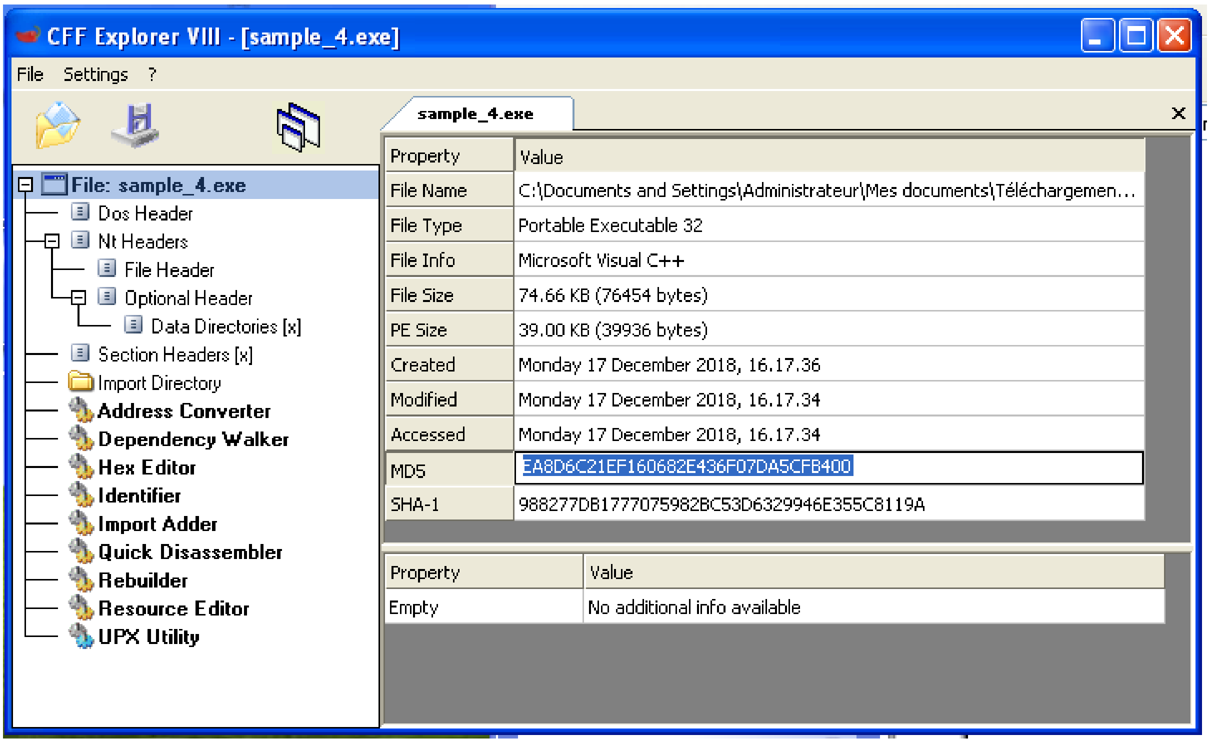
Property	Value
File Name	C:\Documents and Settings\Administrateur\Mes documents\Téléchargemen...
File Type	Portable Executable 32
File Info	Microsoft Visual C++
File Size	74.66 KB (76454 bytes)
PE Size	39.00 KB (39936 bytes)
Created	Monday 17 December 2018, 16.17.36
Modified	Monday 17 December 2018, 16.17.34
Accessed	Monday 17 December 2018, 16.17.34
MD5	EA8D6C21EF160682E436F07DA5CFB400
SHA-1	988277DB1777075982BC53D6329946E355C8119A

Property	Value
Empty	No additional info available

After importing the file in CFF explorer, you can see MD5 and SHA-1 passwords.

Md5:

MD5hashis contain 32 bits and it will display above on SHA-1.



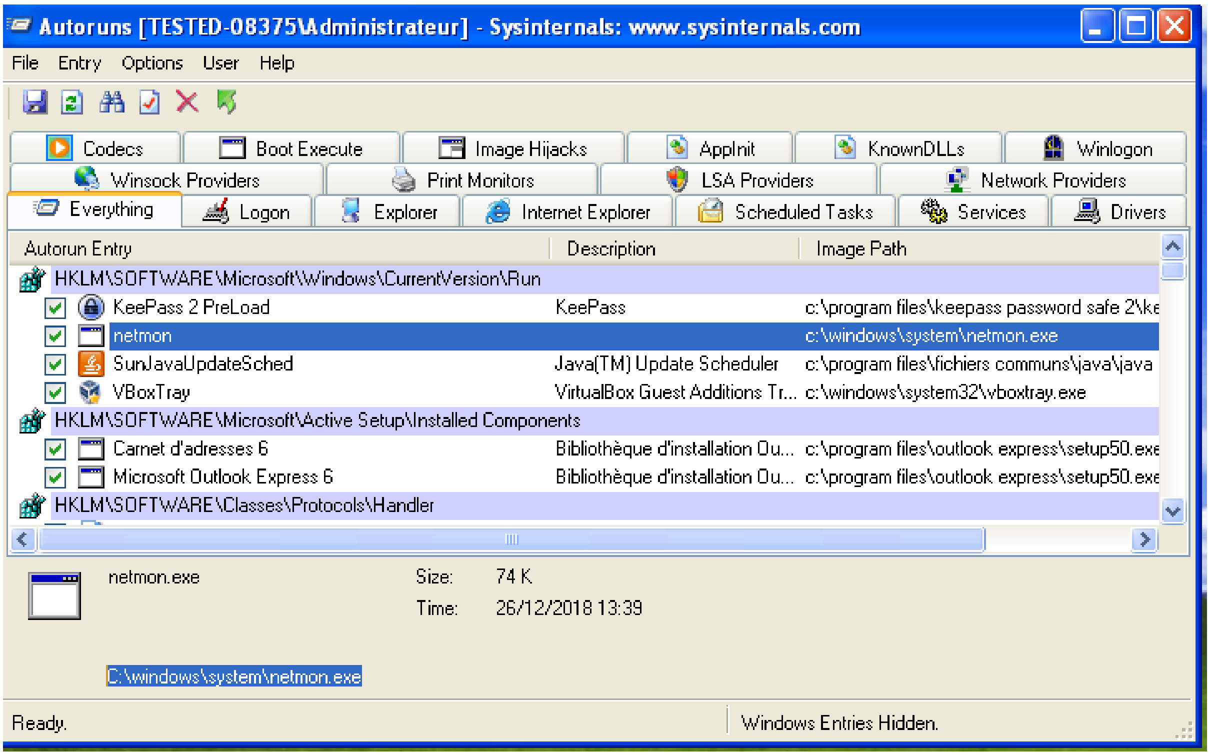
Property	Value
File Name	C:\Documents and Settings\Administrateur\Mes documents\Téléchargemen...
File Type	Portable Executable 32
File Info	Microsoft Visual C++
File Size	74.66 KB (76454 bytes)
PE Size	39.00 KB (39936 bytes)
Created	Monday 17 December 2018, 16.17.36
Modified	Monday 17 December 2018, 16.17.34
Accessed	Monday 17 December 2018, 16.17.34
MD5	EA8D6C21EF160682E436F07DA5CFB400
SHA-1	988277DB1777075982BC53D6329946E355C8119A

Property	Value
Empty	No additional info available

What are the create/dropped files on disk?

=>After downloading file from website, I changed the extension to .exe,

=>When I clicked on malware application, it automatically hides from download folder



Autorun Entry	Description	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run		
☑ KeePass 2 PreLoad	KeePass	c:\program files\keepass password safe 2\ke
☑ netmon		c:\windows\system\netmon.exe
☑ SunJavaUpdateSched	Java(TM) Update Scheduler	c:\program files\fichiers communs\java\java
☑ VBoxTray	VirtualBox Guest Additions Tr...	c:\windows\system32\vboxtray.exe
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components		
☑ Carnet d'adresses 6	Bibliothèque d'installation Ou...	c:\program files\outlook express\setup50.exe
☑ Microsoft Outlook Express 6	Bibliothèque d'installation Ou...	c:\program files\outlook express\setup50.exe
HKLM\SOFTWARE\Classes\Protocols\Handler		

netmon.exe Size: 74 K
Time: 26/12/2018 13:39

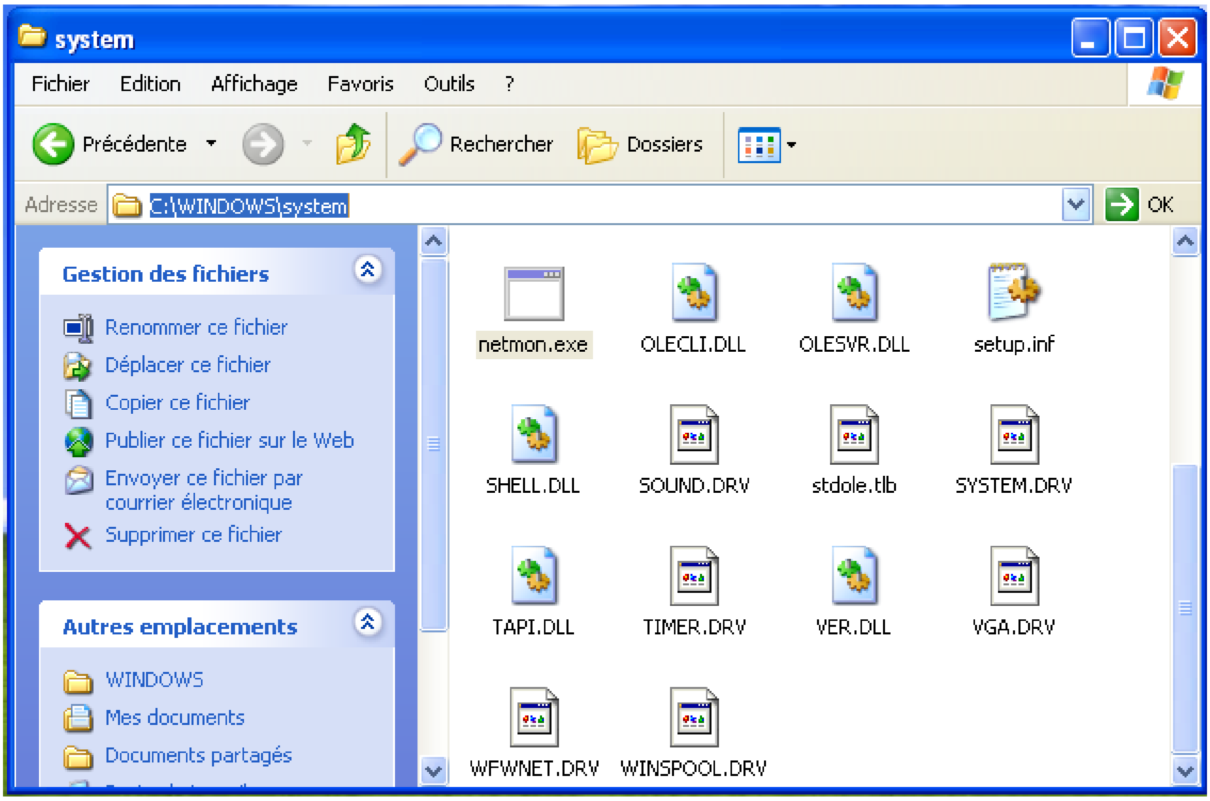
C:\windows\system\netmon.exe

Ready. Windows Entries Hidden.

=>I opened autorun and checked the location.

We can see the netmon.exe file inside the below path.

C:WINDOWS/system/netmon.exe

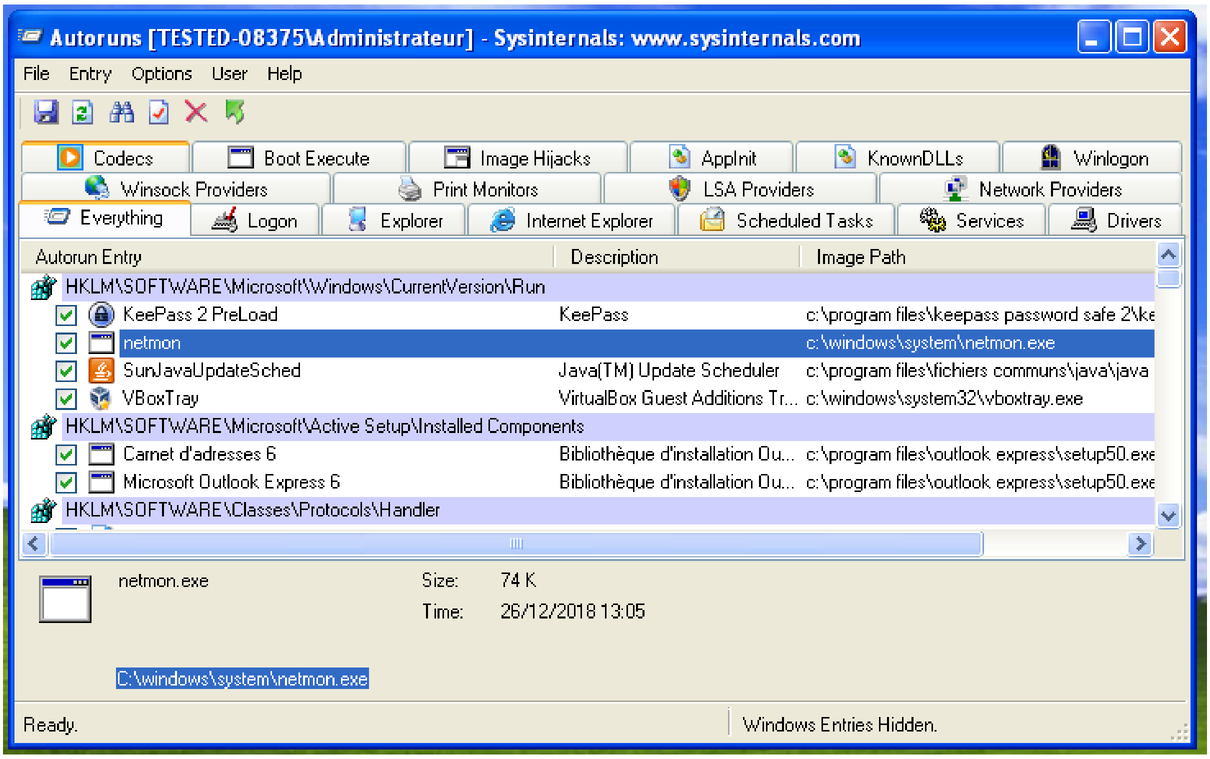

system
Fichier
Edition
Affichage
Favoris
Outils
?
Précédente
Rechercher
Dossiers
Adresse
C:\WINDOWS\system
OK
Gestion des fichiers
Renommer ce fichier
Déplacer ce fichier
Copier ce fichier
Publier ce fichier sur le Web
Envoyer ce fichier par courrier électronique
Supprimer ce fichier
Autres emplacements
WINDOWS
Mes documents
Documents partagés
netmon.exe
OLECLI.DLL
OLESVR.DLL
setup.inf
SHELL.DLL
SOUND.DRV
stdole.tlb
SYSTEM.DRV
TAPI.DLL
TIMER.DRV
VER.DLL
VGA.DRV
WFWNET.DRV
WINSPOOL.DRV

How to clean the system?

netmon.exe is most likely a virus or Trojan, in which case it should be stopped or removed immediately.

To remove this malware from your system, you have to use Autorun software.

After opening this application, you can see the file that look different to you, here I found NetMon file is looks like different and I must delete it.



Autorun Entry	Description	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run		
☑ KeePass 2 PreLoad	KeePass	c:\program files\keepass password safe 2\ke
☑ netmon		c:\windows\system\netmon.exe
☑ SunJavaUpdateSched	Java(TM) Update Scheduler	c:\program files\fichiers communs\java\java
☑ VBoxTray	VirtualBox Guest Additions Tr...	c:\windows\system32\vboxtray.exe
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components		
☑ Carnet d'adresses 6	Bibliothèque d'installation Ou...	c:\program files\outlook express\setup50.exe
☑ Microsoft Outlook Express 6	Bibliothèque d'installation Ou...	c:\program files\outlook express\setup50.exe
HKLM\SOFTWARE\Classes\Protocols\Handler		

netmon.exe

Size: 74 K

Time: 26/12/2018 13:05

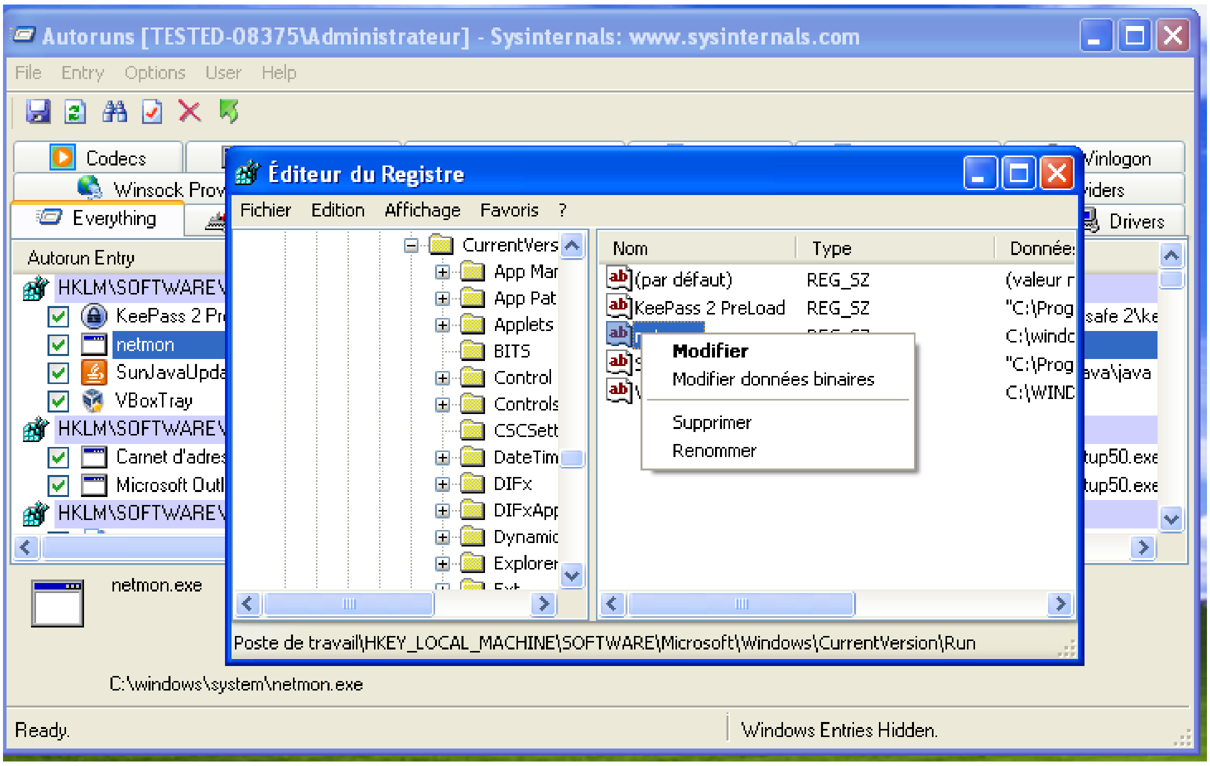
C:\windows\system\netmon.exe

Ready.

Windows Entries Hidden.

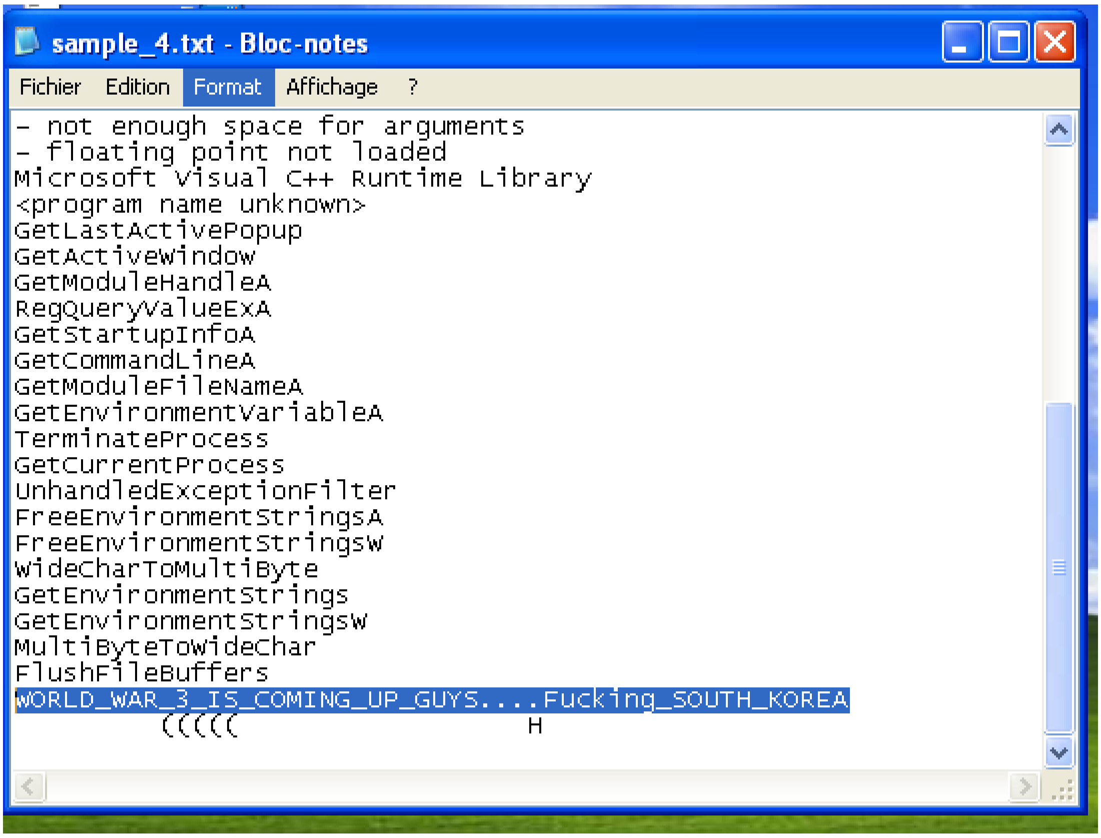
You can remove this file by using 2 steps, First one, you can right click on malware file and you can see the options for delete, click on delete and the malware is deleted from your system

Second one, you can double click on malware and it will display below screenshot.



Right click on netmon folder and it will display some option, click on supprimer, this malware will remove from your system.

Finally, I Found for this netmon.exe file contain secret information,



```
- not enough space for arguments
- floating point not loaded
Microsoft Visual C++ Runtime Library
<program name unknown>
GetLastActivePopup
GetActiveWindow
GetModuleHandleA
RegQueryValueExA
GetStartupInfoA
GetCommandLineA
GetModuleFileNameA
GetEnvironmentVariableA
TerminateProcess
GetCurrentProcess
UnhandledExceptionFilter
FreeEnvironmentStringsA
FreeEnvironmentStringsW
WideCharToMultiByte
GetEnvironmentStrings
GetEnvironmentStringsW
MultiByteToWideChar
FlushFileBuffers
WORLD_WAR_3_IS_COMING_UP_GUYS....Fucking_SOUTH_KOREA
         (((((                  H
```

This is the end of the report