MALWARE ANALYSIS

Prof. Adel KHALDI

By,

Min-ji Choi(Exchange student)

Raymond ZALOUM M.E (SNS)

Bharani MOORTHY M.E (SNS)

INDEX

SYNTHESIS

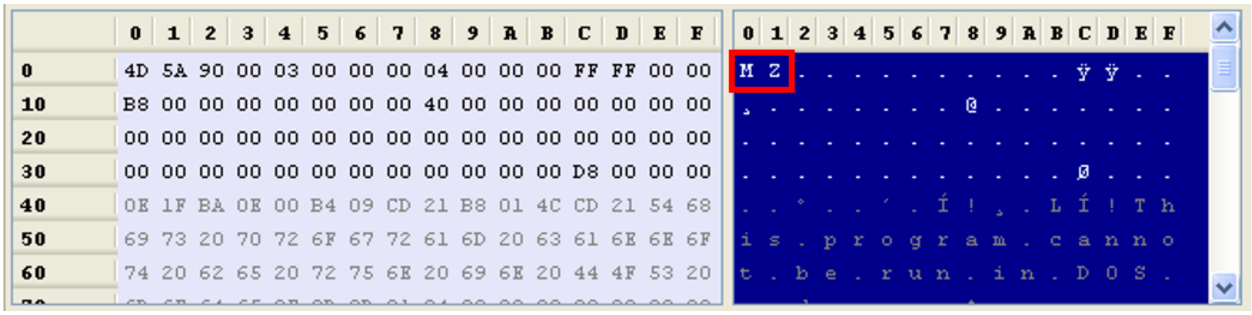
We downloaded the malware file sample_7_exam.html and renamed into .exe and started both static and dynamic analysis part, we found that the malware deletes its source location and creates another file names netmon.exe and it makes remote communication to the computer residing in the local network via 445 port (Eternal Blue – used the same exploit !).We found most interesting things in memory analysis. Putting it All together, we used the tools such as procmon, procexp, wireshark, dumpit and volatility to detect the malware and its intention.

IDENTIFICATION

We used the Static Analysis and found the details of the malware sample as follows:

1. **File type**

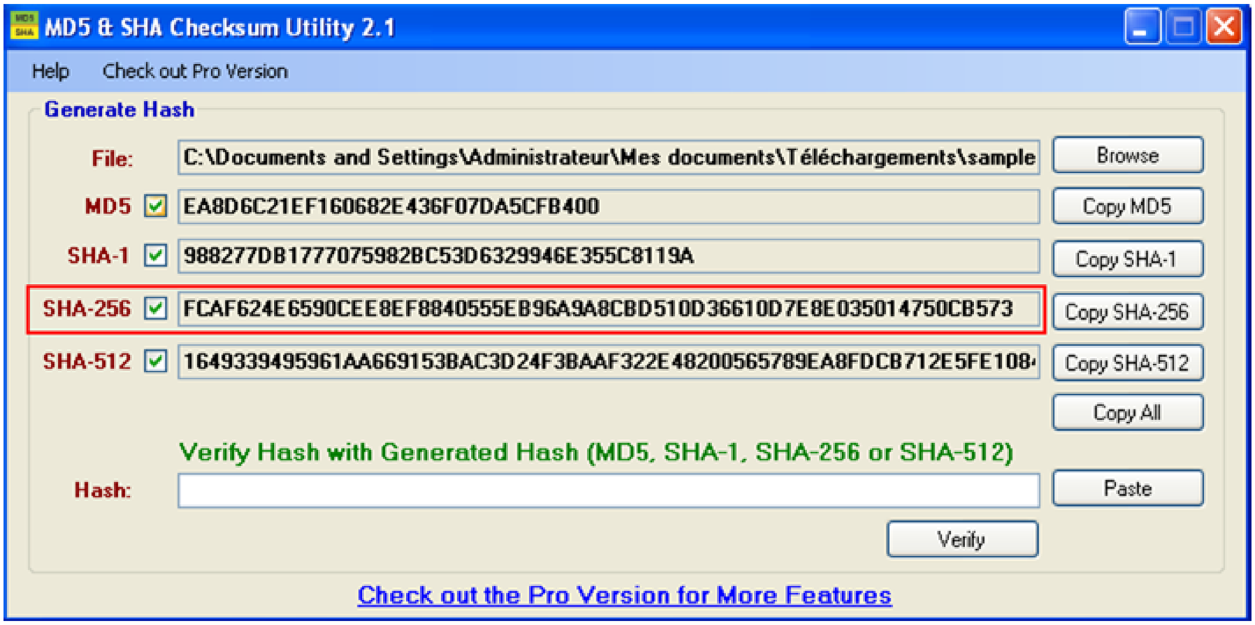
We have found our downloaded malware file is.EXE format by examining the magic bytes in PE bear.



```
     0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F    0 1 2 3 4 5 6 7 8 9 A B C D E F
0    4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00   M Z . . . . . . . . . . ÿ ÿ . .
10   B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ¸ . . . . . . . @ . . . . . . .
20   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   . . . . . . . . . . . . . . . .
30   00 00 00 00 00 00 00 00 00 00 00 00 D8 00 00 00   . . . . . . . . . . . . Ø . . .
40   0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68   . . º . . ´ . Í ! ¸ . L Í ! T h
50   69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F   i s . p r o g r a m . c a n n o
60   74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20   t . b e . r u n . i n . D O S .
```

2. **File Hash**

The below file Hashed has found using the MD5 & SHA Checksum Utility.



MD5 & SHA Checksum Utility 2.1

Help   Check out Pro Version

Generate Hash

File: C:\Documents and Settings\Administrateur\Mes documents\Téléchargements\sample

MD5 ☑ EA8D6C21EF160682E436F07DA5CFB400

SHA-1 ☑ 988277DB1777075982BC53D6329946E355C8119A

SHA-256 ☑ FCAF624E6590CEE8EF8840555EB96A9A8CBD510D36610D7E8E035014750CB573

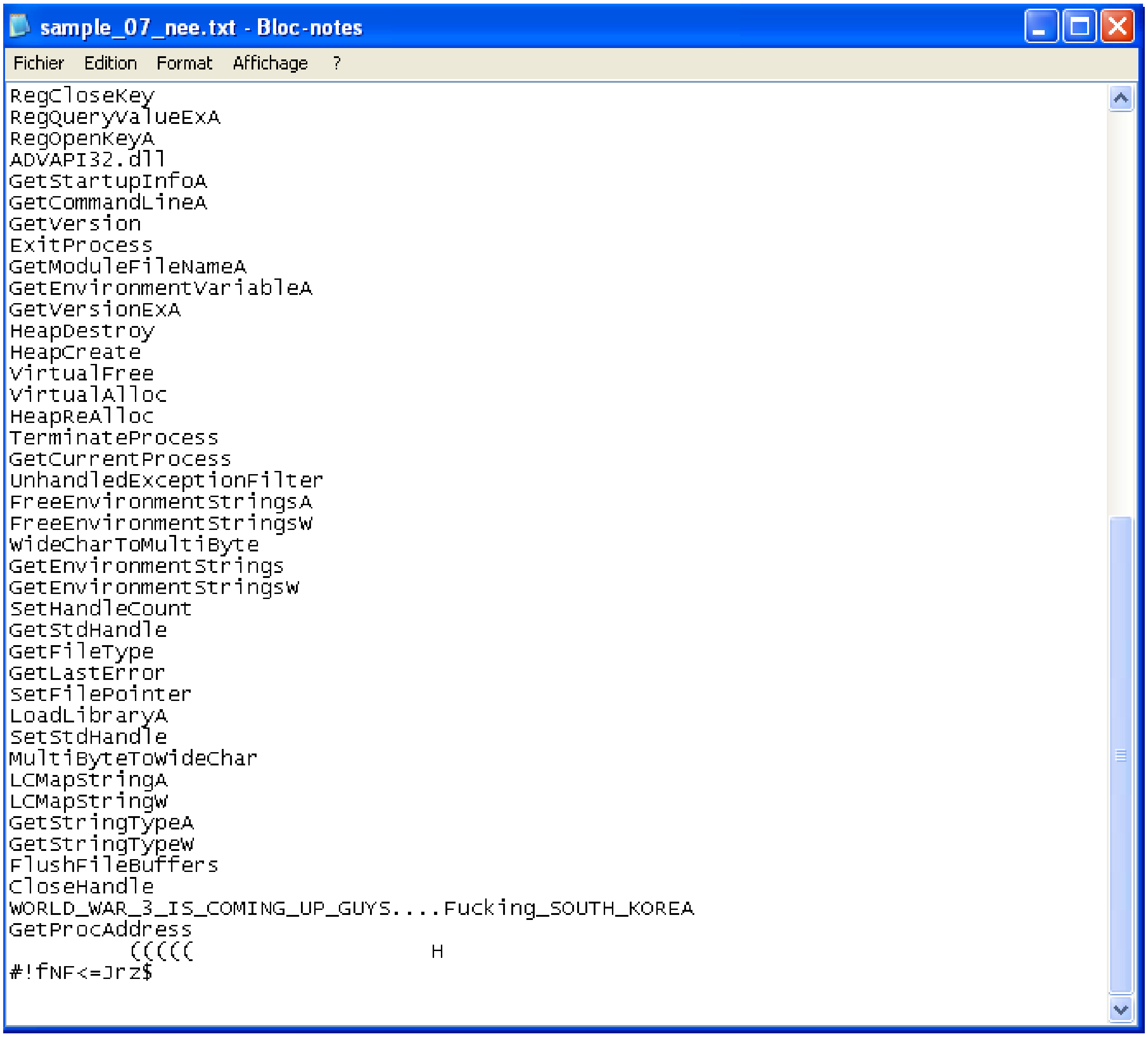
SHA-512 ☑ 1649339495961AA669153BAC3D24F3BAAF322E48200565789EA8FDCB712E5FE108

Verify Hash with Generated Hash (MD5, SHA-1, SHA-256 or SHA-512)

Hash:

3. **Strings**

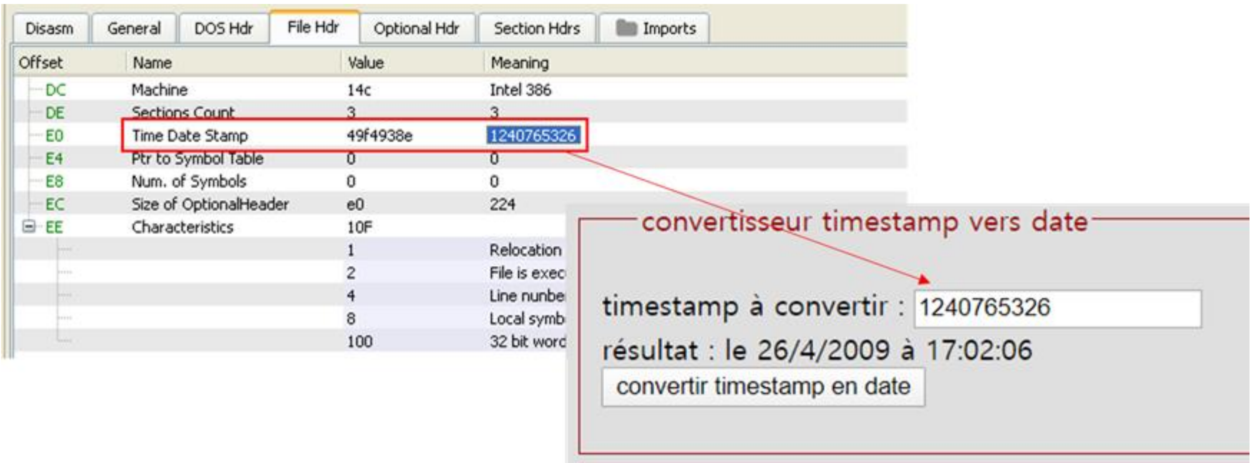
We have exported the strings in downloaded software using strings tool and found some interesting strings as follows:
ExitProcess
TerminateProcess
*.dll files like: user32.dll, KERNEL32.dll , ADVAPI32.dll



```
RegCloseKey
RegQueryValueExA
RegOpenKeyA
ADVAPI32.dll
GetStartupInfoA
GetCommandLineA
GetVersion
ExitProcess
GetModuleFileNameA
GetEnvironmentVariableA
GetVersionExA
HeapDestroy
HeapCreate
VirtualFree
VirtualAlloc
HeapReAlloc
TerminateProcess
GetCurrentProcess
UnhandledExceptionFilter
FreeEnvironmentStringsA
FreeEnvironmentStringsW
WideCharToMultiByte
GetEnvironmentStrings
GetEnvironmentStringsW
SetHandleCount
GetStdHandle
GetFileType
GetLastError
SetFilePointer
LoadLibraryA
SetStdHandle
MultiByteToWideChar
LCMapStringA
LCMapStringW
GetStringTypeA
GetStringTypeW
FlushFileBuffers
CloseHandle
WORLD_WAR_3_IS_COMING_UP_GUYS....Fucking_SOUTH_KOREA
GetProcAddress
         (((((                  H
#!fNF<=Jrz$
```

4.Compilation date

We have found that the compilation date of the downloaded software is April 26th, 2009 at 17:02:06 according to PE bear and online timestamp calculator.



Offset	Name	Value	Meaning
DC	Machine	14c	Intel 386
DE	Sections Count	3	3
E0	Time Date Stamp	49f4938e	1240765326
E4	Ptr to Symbol Table	0	0
E8	Num. of Symbols	0	0
EC	Size of OptionalHeader	e0	224
EE	Characteristics	10F	
		1	Relocation
		2	File is exec
		4	Line nunbe
		8	Local symb
		100	32 bit word

convertisseur timestamp vers date

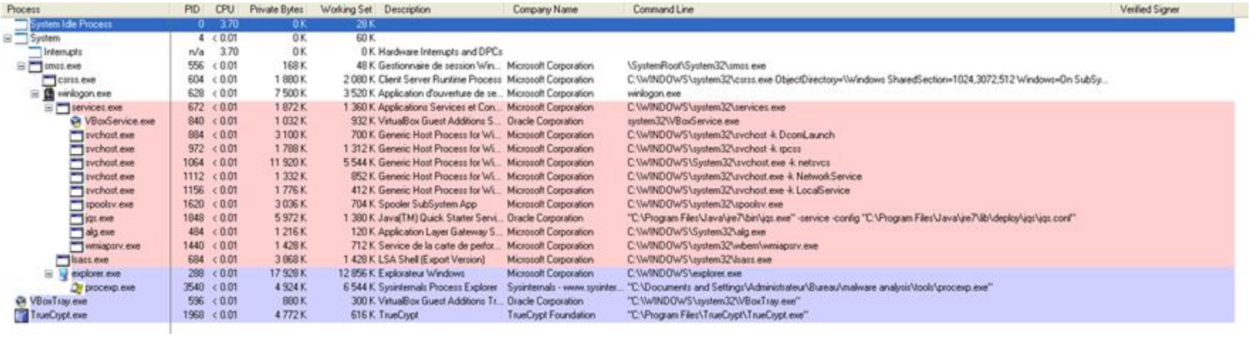
timestamp à convertir : 1240765326

résultat : le 26/4/2009 à 17:02:06

DYNAMIC ANALYSIS

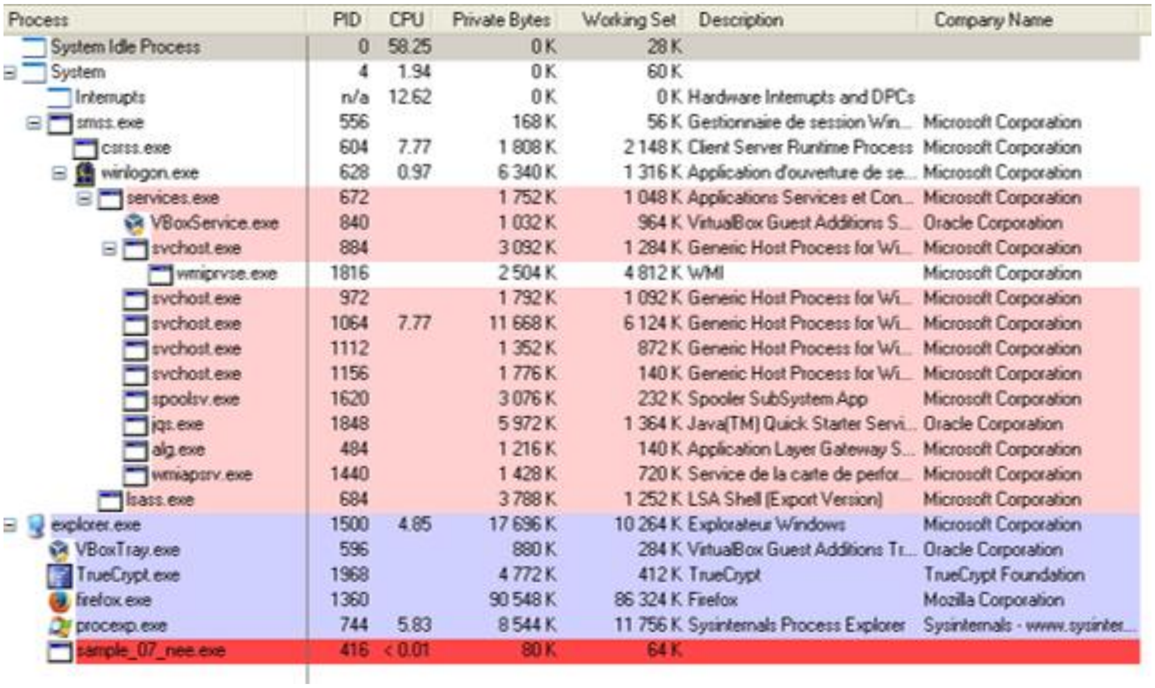
1. Process Explorer

We couldn’t find any other information by Process Explorer rather than the fact that the malware is executed.



Process	PID	CPU	Private Bytes	Working Set	Description	Company Name	Command Line	Verified Signer
System Idle Process	0	3.70	0 K	28 K				
System	4	< 0.01	0 K	60 K				
Interrupts	n/a	3.70	0 K	0 K	Hardware Interrupts and DPCs			
smss.exe	556	< 0.01	168 K	48 K	Gestionnaire de session Win...	Microsoft Corporation	\SystemRoot\System32\smss.exe	
csrss.exe	604	< 0.01	1 880 K	2 080 K	Client Server Runtime Process	Microsoft Corporation	C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSy...	
winlogon.exe	628	< 0.01	7 500 K	3 520 K	Application d'ouverture de se...	Microsoft Corporation	winlogon.exe	
services.exe	672	< 0.01	1 872 K	1 360 K	Applications Services et Con...	Microsoft Corporation	C:\WINDOWS\system32\services.exe	
VBoxService.exe	840	< 0.01	1 032 K	932 K	VirtualBox Guest Additions S...	Oracle Corporation	system32\VBoxService.exe	
svchost.exe	884	< 0.01	3 100 K	700 K	Generic Host Process for Wi...	Microsoft Corporation	C:\WINDOWS\system32\svchost -k DcomLaunch	
svchost.exe	972	< 0.01	1 788 K	1 312 K	Generic Host Process for Wi...	Microsoft Corporation	C:\WINDOWS\system32\svchost -k rpcss	
svchost.exe	1064	< 0.01	11 920 K	5 544 K	Generic Host Process for Wi...	Microsoft Corporation	C:\WINDOWS\System32\svchost.exe -k netsvcs	
svchost.exe	1112	< 0.01	1 332 K	852 K	Generic Host Process for Wi...	Microsoft Corporation	C:\WINDOWS\system32\svchost.exe -k NetworkService	
svchost.exe	1156	< 0.01	1 776 K	412 K	Generic Host Process for Wi...	Microsoft Corporation	C:\WINDOWS\system32\svchost.exe -k LocalService	
spoolsv.exe	1620	< 0.01	3 036 K	704 K	Spooler SubSystem App	Microsoft Corporation	C:\WINDOWS\system32\spoolsv.exe	
jqs.exe	1848	< 0.01	5 972 K	1 380 K	Java(TM) Quick Starter Servi...	Oracle Corporation	"C:\Program Files\Java\jre7\bin\jqs.exe" -service -config "C:\Program Files\Java\jre7\lib\deploy\jqs\jqs.conf"	
alg.exe	484	< 0.01	1 216 K	120 K	Application Layer Gateway S...	Microsoft Corporation	C:\WINDOWS\System32\alg.exe	
wmiapsrv.exe	1440	< 0.01	1 428 K	712 K	Service de la carte de perfor...	Microsoft Corporation	C:\WINDOWS\system32\wbem\wmiapsrv.exe	
lsass.exe	684	< 0.01	3 868 K	1 428 K	LSA Shell (Export Version)	Microsoft Corporation	C:\WINDOWS\system32\lsass.exe	
explorer.exe	288	< 0.01	17 928 K	12 856 K	Explorateur Windows	Microsoft Corporation	C:\WINDOWS\explorer.exe	
procexp.exe	3540	< 0.01	4 924 K	6 544 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...	"C:\Documents and Settings\Administrateur\Bureau\malware analysis\tools\procexp.exe"	
VBoxTray.exe	596	< 0.01	880 K	300 K	VirtualBox Guest Additions Tr...	Oracle Corporation	"C:\WINDOWS\system32\VBoxTray.exe"	
TrueCrypt.exe	1968	< 0.01	4 772 K	616 K	TrueCrypt	TrueCrypt Foundation	"C:\Program Files\TrueCrypt\TrueCrypt.exe"	

Screenshot before executing the malware



Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	58.25	0 K	28 K		
System	4	1.94	0 K	60 K		
Interrupts	n/a	12.62	0 K	0 K	Hardware Interrupts and DPCs	
smss.exe	556		168 K	56 K	Gestionnaire de session Win...	Microsoft Corporation
csrss.exe	604	7.77	1 808 K	2 148 K	Client Server Runtime Process	Microsoft Corporation
winlogon.exe	628	0.97	6 340 K	1 316 K	Application d'ouverture de se...	Microsoft Corporation
services.exe	672		1 752 K	1 048 K	Applications Services et Con...	Microsoft Corporation
VBoxService.exe	840		1 032 K	964 K	VirtualBox Guest Additions S...	Oracle Corporation
svchost.exe	884		3 092 K	1 284 K	Generic Host Process for Wi...	Microsoft Corporation
wmiprvse.exe	1816		2 504 K	4 812 K	WMI	Microsoft Corporation
svchost.exe	972		1 792 K	1 092 K	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1064	7.77	11 668 K	6 124 K	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1112		1 352 K	872 K	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1156		1 776 K	140 K	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe	1620		3 076 K	232 K	Spooler SubSystem App	Microsoft Corporation
jqs.exe	1848		5 972 K	1 364 K	Java(TM) Quick Starter Servi...	Oracle Corporation
alg.exe	484		1 216 K	140 K	Application Layer Gateway S...	Microsoft Corporation
wmiapsrv.exe	1440		1 428 K	720 K	Service de la carte de perfor...	Microsoft Corporation
lsass.exe	684		3 788 K	1 252 K	LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	1500	4.85	17 696 K	10 264 K	Explorateur Windows	Microsoft Corporation
VBoxTray.exe	596		880 K	284 K	VirtualBox Guest Additions Tr...	Oracle Corporation
TrueCrypt.exe	1968		4 772 K	412 K	TrueCrypt	TrueCrypt Foundation
firefox.exe	1360		90 548 K	86 324 K	Firefox	Mozilla Corporation
procexp.exe	744	5.83	8 544 K	11 756 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
sample_07_nee.exe	416	< 0.01	80 K	64 K		

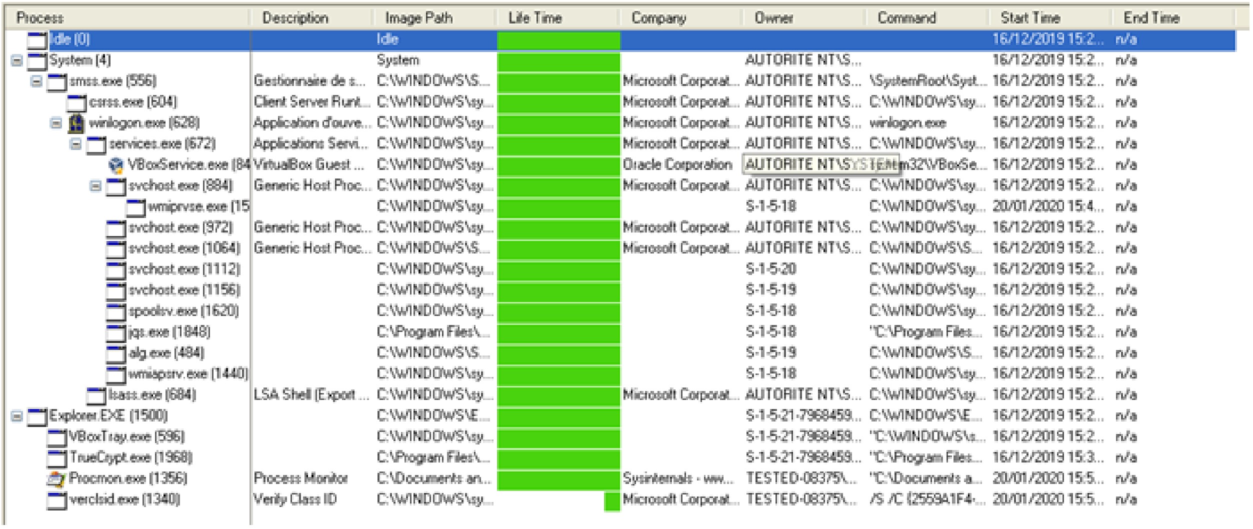
Screenshot after executing the malware

2. Process Monitor

We have found that the malware is also executing the other program according to Process Monitor. The file path of the executed programs is→*C:\Windows\system\netmon.exe*.

In addition, the program *cmd* is also executed for deleting the malware itself.

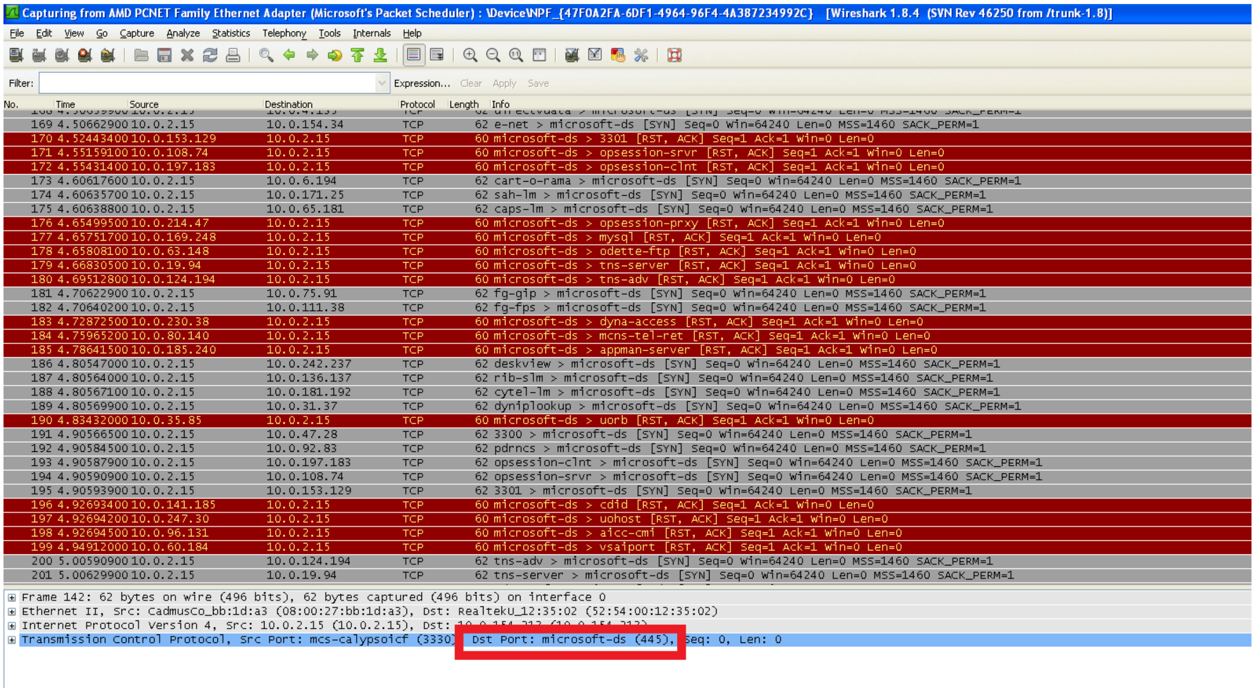
Screenshot before executing the malware:



Process	Description	Image Path	Life Time	Company	Owner	Command	Start Time	End Time
Idle (0)		Idle	🟩				16/12/2019 15:2...	n/a
System (4)		System	🟩		AUTORITE NT\S...		16/12/2019 15:2...	n/a
smss.exe (556)	Gestionnaire de s...	C:\WINDOWS\S...	🟩	Microsoft Corporat...	AUTORITE NT\S...	\SystemRoot\Syst...	16/12/2019 15:2...	n/a
csrss.exe (604)	Client Server Runt...	C:\WINDOWS\sy...	🟩	Microsoft Corporat...	AUTORITE NT\S...	C:\WINDOWS\sy...	16/12/2019 15:2...	n/a
winlogon.exe (628)	Application d'ouve...	C:\WINDOWS\sy...	🟩	Microsoft Corporat...	AUTORITE NT\S...	winlogon.exe	16/12/2019 15:2...	n/a
services.exe (672)	Applications Servi...	C:\WINDOWS\sy...	🟩	Microsoft Corporat...	AUTORITE NT\S...	C:\WINDOWS\sy...	16/12/2019 15:2...	n/a
VBoxService.exe (84	VirtualBox Guest ...	C:\WINDOWS\sy...	🟩	Oracle Corporation	AUTORITE NT\SYSTEM	m32\VBoxSe...	16/12/2019 15:2...	n/a
svchost.exe (884)	Generic Host Proc...	C:\WINDOWS\sy...	🟩	Microsoft Corporat...	AUTORITE NT\S...	C:\WINDOWS\sy...	16/12/2019 15:2...	n/a
wmiprvse.exe (15		C:\WINDOWS\sy...	🟩		S-1-5-18	C:\WINDOWS\sy...	20/01/2020 15:4...	n/a
svchost.exe (972)	Generic Host Proc...	C:\WINDOWS\sy...	🟩	Microsoft Corporat...	AUTORITE NT\S...	C:\WINDOWS\sy...	16/12/2019 15:2...	n/a
svchost.exe (1064)	Generic Host Proc...	C:\WINDOWS\S...	🟩	Microsoft Corporat...	AUTORITE NT\S...	C:\WINDOWS\S...	16/12/2019 15:2...	n/a
svchost.exe (1112)		C:\WINDOWS\sy...	🟩		S-1-5-20	C:\WINDOWS\sy...	16/12/2019 15:2...	n/a
svchost.exe (1156)		C:\WINDOWS\sy...	🟩		S-1-5-19	C:\WINDOWS\sy...	16/12/2019 15:2...	n/a
spoolsv.exe (1620)		C:\WINDOWS\sy...	🟩		S-1-5-18	C:\WINDOWS\sy...	16/12/2019 15:2...	n/a
jqs.exe (1848)		C:\Program Files\...	🟩		S-1-5-18	"C:\Program Files...	16/12/2019 15:2...	n/a
alg.exe (484)		C:\WINDOWS\S...	🟩		S-1-5-19	C:\WINDOWS\S...	16/12/2019 15:2...	n/a
wmiapsrv.exe (1440)		C:\WINDOWS\sy...	🟩		S-1-5-18	C:\WINDOWS\sy...	16/12/2019 15:2...	n/a
lsass.exe (684)	LSA Shell (Export ...	C:\WINDOWS\sy...	🟩	Microsoft Corporat...	AUTORITE NT\S...	C:\WINDOWS\sy...	16/12/2019 15:2...	n/a
Explorer.EXE (1500)		C:\WINDOWS\E...	🟩		S-1-5-21-7968459...	C:\WINDOWS\E...	16/12/2019 15:2...	n/a
VBoxTray.exe (596)		C:\WINDOWS\sy...	🟩		S-1-5-21-7968459...	"C:\WINDOWS\s...	16/12/2019 15:2...	n/a
TrueCrypt.exe (1968)		C:\Program Files\...	🟩		S-1-5-21-7968459...	"C:\Program Files...	16/12/2019 15:3...	n/a
Procmon.exe (1356)	Process Monitor	C:\Documents an...	🟩	Sysinternals - ww...	TESTED-08375\...	"C:\Documents a...	20/01/2020 15:5...	n/a
verclsid.exe (1340)	Verify Class ID	C:\WINDOWS\sy...	🟩	Microsoft Corporat...	TESTED-08375\...	/S /C {2559A1F4-...	20/01/2020 15:5...	n/a

Screenshot after executing the malware:

3. Network traffic Analysis by Wireshark:


Capturing from AMD PCNET Family Ethernet Adapter (Microsoft's Packet Scheduler) : \Device\NPF_{47F0A2FA-6DF1-4964-96F4-4A387234992C} [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time        Source         Destination    Protocol Length Info
 169 4.50662900 10.0.2.15      10.0.154.34    TCP   62 e-net > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 170 4.52443400 10.0.153.129   10.0.2.15      TCP   60 microsoft-ds > 3301 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 171 4.55159100 10.0.108.74    10.0.2.15      TCP   60 microsoft-ds > opsession-srvr [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 172 4.55431400 10.0.197.183   10.0.2.15      TCP   60 microsoft-ds > opsession-clnt [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 173 4.60617600 10.0.2.15      10.0.6.194     TCP   62 cart-o-rama > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 174 4.60635700 10.0.2.15      10.0.171.25    TCP   62 sah-lm > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 175 4.60638800 10.0.2.15      10.0.65.181    TCP   62 caps-lm > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 176 4.65499500 10.0.214.47    10.0.2.15      TCP   60 microsoft-ds > opsession-prxy [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 177 4.65751700 10.0.169.248   10.0.2.15      TCP   60 microsoft-ds > mysql [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 178 4.65808100 10.0.63.148    10.0.2.15      TCP   60 microsoft-ds > odette-ftp [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 179 4.66830500 10.0.19.94     10.0.2.15      TCP   60 microsoft-ds > tns-server [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 180 4.69512800 10.0.124.194   10.0.2.15      TCP   60 microsoft-ds > tns-adv [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 181 4.70622900 10.0.2.15      10.0.75.91     TCP   62 fg-gip > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 182 4.70640200 10.0.2.15      10.0.111.38    TCP   62 fg-fps > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 183 4.72872500 10.0.230.38    10.0.2.15      TCP   60 microsoft-ds > dyna-access [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 184 4.75965200 10.0.80.140    10.0.2.15      TCP   60 microsoft-ds > mcns-tel-ret [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 185 4.78641500 10.0.185.240   10.0.2.15      TCP   60 microsoft-ds > appman-server [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 186 4.80547000 10.0.2.15      10.0.242.237   TCP   62 deskview > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 187 4.80564000 10.0.2.15      10.0.136.137   TCP   62 rib-slm > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 188 4.80567100 10.0.2.15      10.0.181.192   TCP   62 cytel-lm > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 189 4.80569900 10.0.2.15      10.0.31.37     TCP   62 dyniplookup > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 190 4.83432000 10.0.35.85     10.0.2.15      TCP   60 microsoft-ds > uorb [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 191 4.90566500 10.0.2.15      10.0.47.28     TCP   62 3300 > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 192 4.90584500 10.0.2.15      10.0.92.83     TCP   62 pdrncs > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 193 4.90587900 10.0.2.15      10.0.197.183   TCP   62 opsession-clnt > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 194 4.90590900 10.0.2.15      10.0.108.74    TCP   62 opsession-srvr > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 195 4.90593900 10.0.2.15      10.0.153.129   TCP   62 3301 > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 196 4.92693400 10.0.141.185   10.0.2.15      TCP   60 microsoft-ds > cdid [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 197 4.92694200 10.0.247.30    10.0.2.15      TCP   60 microsoft-ds > uohost [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 198 4.92694500 10.0.96.131    10.0.2.15      TCP   60 microsoft-ds > aicc-cmi [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 199 4.94912000 10.0.60.184    10.0.2.15      TCP   60 microsoft-ds > vsaiport [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 200 5.00590900 10.0.2.15      10.0.124.194   TCP   62 tns-adv > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 201 5.00629900 10.0.2.15      10.0.19.94     TCP   62 tns-server > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1

⊞ Frame 142: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
⊞ Ethernet II, Src: CadmusCo_bb:1d:a3 (08:00:27:bb:1d:a3), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
⊞ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 10.0.154.213 (10.0.154.213)
⊞ Transmission Control Protocol, Src Port: mcs-calypsoicf (3330), Dst Port: microsoft-ds (445), Seq: 0, Len: 0
```

We have analysed the network traffic to find the malware is making any network communication to other networks/ local network.

Firstly, it seems that the malware is brute forcing within the network with port number 445 (SMB)

- ➔ Now, we got the flashback of the great ransomware attack named ***Wannacry /EternalBlue*** used the same windows Port 445 vulnerability -Server Message Block where application can read, create and update files on the remote server. The malware is trying to scan all computers in the network.

- ➔ Suppose that the malware finds a port 445 open in a computer, then the malware can CRUD operation (Create , read , update and delete).

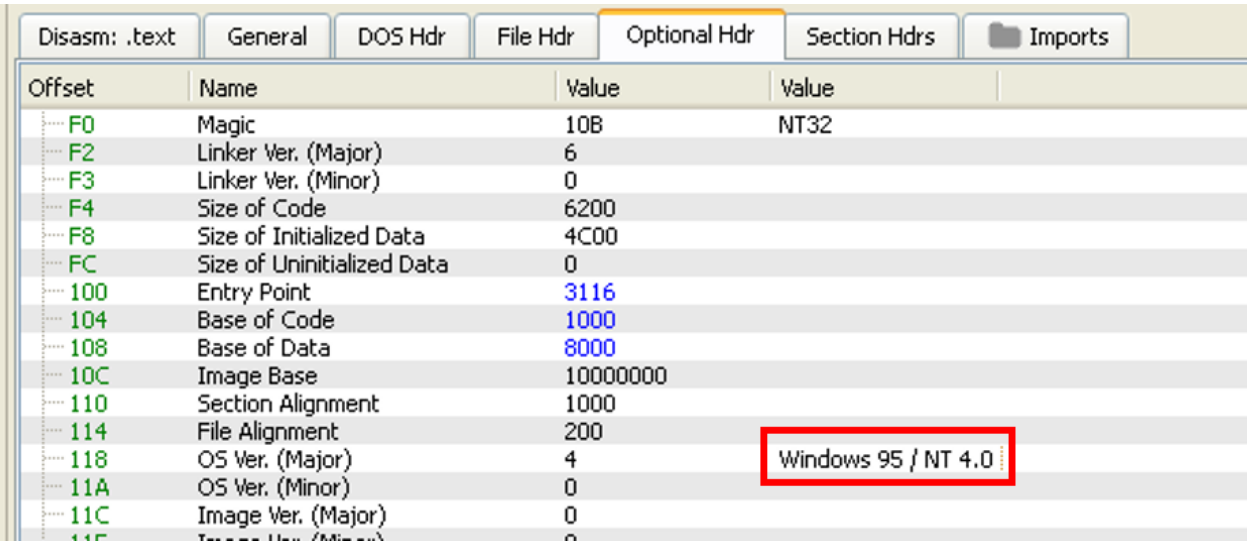
- ➔ https://www.altospam.com/actualite/2017/05/attaque-wannacry-via-smb-jaff-email/

MEMORY FORENSICS ANALYSIS

For the memory analysis, we used an indispensable tool name **volatility** (which we have taught to us in windows forensics class) to analysis the dumped file.

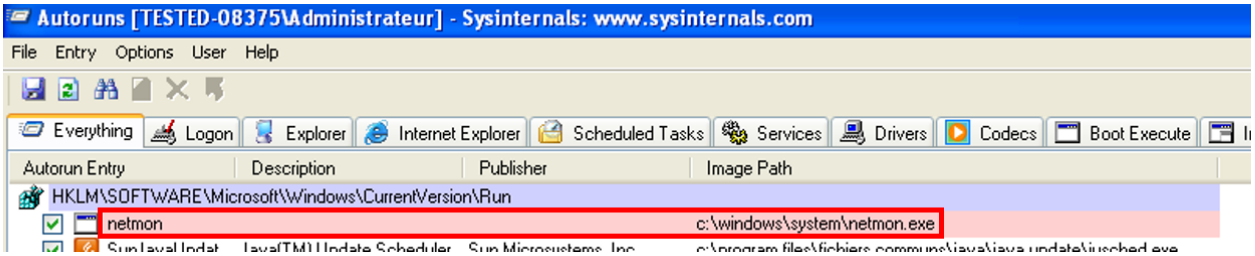
1- **From which operating system's version this image was taken?**

The file has been analyzed via PEbear and we found that the image was taken in Windows 95 Operating system.



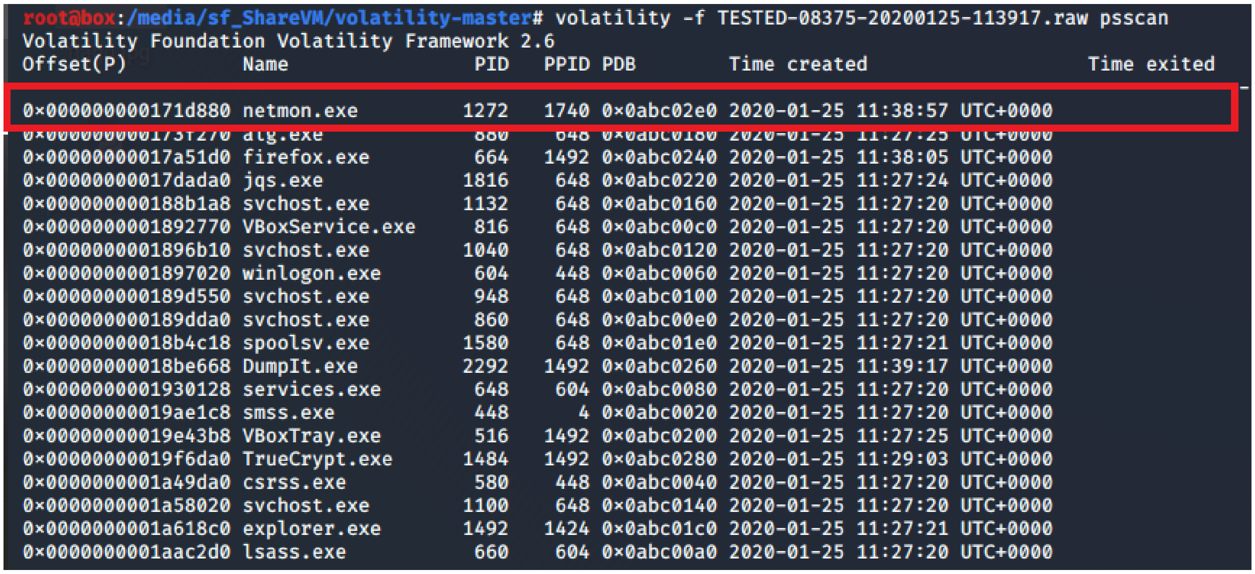
Offset	Name	Value	Value
F0	Magic	10B	NT32
F2	Linker Ver. (Major)	6	
F3	Linker Ver. (Minor)	0	
F4	Size of Code	6200	
F8	Size of Initialized Data	4C00	
FC	Size of Uninitialized Data	0	
100	Entry Point	3116	
104	Base of Code	1000	
108	Base of Data	8000	
10C	Image Base	10000000	
110	Section Alignment	1000	
114	File Alignment	200	
118	OS Ver. (Major)	4	Windows 95 / NT 4.0
11A	OS Ver. (Minor)	0	
11C	Image Ver. (Major)	0	
11E	Image Ver. (Minor)	0	

2- **What are the strange processes? Are they malicious? Why?**


Autoruns [TESTED-08375\Administrateur] - Sysinternals: www.sysinternals.com

Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ netmon			c:\windows\system\netmon.exe
☑ SunJavaUpdat	Java(TM) Update Scheduler	Sun Microsystems, Inc.	c:\program files\fichiers communs\java\java update\jusched.exe

Screenshot taken in Autoruns



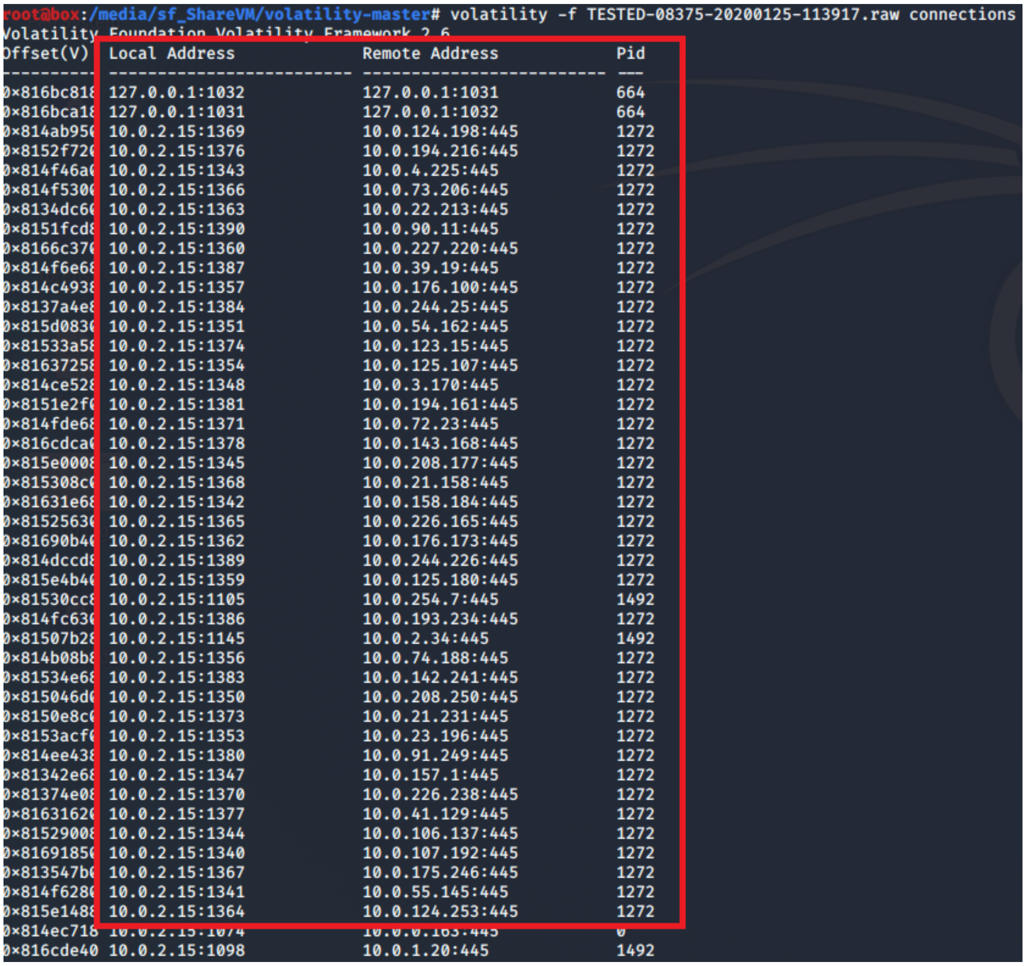
```
root@box:/media/sf_ShareVM/volatility-master# volatility -f TESTED-08375-20200125-113917.raw psscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                PID   PPID PDB        Time created                   Time exited

0x000000000171d880 netmon.exe         1272   1740 0x0abc02e0 2020-01-25 11:38:57 UTC+0000
0x000000000173f270 alg.exe             880    648 0x0abc0180 2020-01-25 11:27:25 UTC+0000
0x00000000017a51d0 firefox.exe         664   1492 0x0abc0240 2020-01-25 11:38:05 UTC+0000
0x00000000017dada0 jqs.exe            1816    648 0x0abc0220 2020-01-25 11:27:24 UTC+0000
0x000000000188b1a8 svchost.exe        1132    648 0x0abc0160 2020-01-25 11:27:20 UTC+0000
0x0000000001892770 VBoxService.exe     816    648 0x0abc00c0 2020-01-25 11:27:20 UTC+0000
0x0000000001896b10 svchost.exe        1040    648 0x0abc0120 2020-01-25 11:27:20 UTC+0000
0x0000000001897020 winlogon.exe        604    448 0x0abc0060 2020-01-25 11:27:20 UTC+0000
0x000000000189d550 svchost.exe         948    648 0x0abc0100 2020-01-25 11:27:20 UTC+0000
0x000000000189dda0 svchost.exe         860    648 0x0abc00e0 2020-01-25 11:27:20 UTC+0000
0x00000000018b4c18 spoolsv.exe        1580    648 0x0abc01e0 2020-01-25 11:27:21 UTC+0000
0x00000000018be668 DumpIt.exe         2292   1492 0x0abc0260 2020-01-25 11:39:17 UTC+0000
0x0000000001930128 services.exe        648    604 0x0abc0080 2020-01-25 11:27:20 UTC+0000
0x00000000019ae1c8 smss.exe            448      4 0x0abc0020 2020-01-25 11:27:20 UTC+0000
0x00000000019e43b8 VBoxTray.exe        516   1492 0x0abc0200 2020-01-25 11:27:25 UTC+0000
0x00000000019f6da0 TrueCrypt.exe      1484   1492 0x0abc0280 2020-01-25 11:29:03 UTC+0000
0x0000000001a49da0 csrss.exe           580    448 0x0abc0040 2020-01-25 11:27:20 UTC+0000
0x0000000001a58020 svchost.exe        1100    648 0x0abc0140 2020-01-25 11:27:20 UTC+0000
0x0000000001a618c0 explorer.exe       1492   1424 0x0abc01c0 2020-01-25 11:27:21 UTC+0000
0x0000000001aac2d0 lsass.exe           660    604 0x0abc00a0 2020-01-25 11:27:20 UTC+0000
```

Screenshot taken in Volatility of netmon.exe and its Pid 1272

- ➔ Yes, there is a strange process that the original malware file named - *sample_07_nee.exe*
- ➔ Creates another file named netmon.exe file and the original file was deleted in order to hide the visibility of the source file identification.
- ➔ Of course, it is **malicious!** we compared the strings of both sample07.exe and netmon.exe – exactly the sale content.
- ➔ Yes, it initiates the brute force attack via port 445 – SMB port in order to propagates / share the malicious file to local machines.

3- **Which process is making network connections?**

. netmon is the process (Pid - 1247) which makes the network communication via port 445 SMB , we can see the similarity in its Pid.

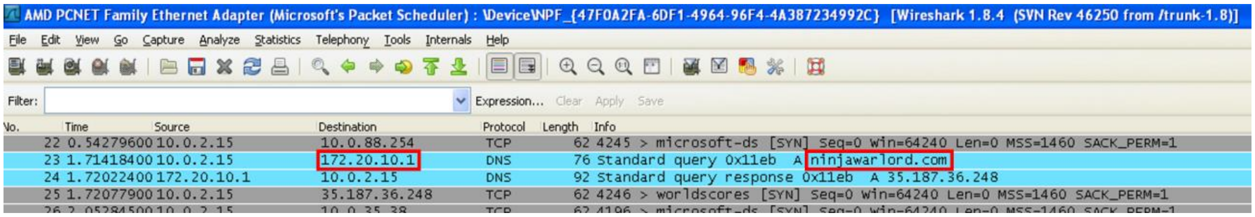


```
root@box:/media/sf_ShareVM/volatility-master# volatility -f TESTED-08375-20200125-113917.raw connections
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x816bc818 127.0.0.1:1032            127.0.0.1:1031            664
0x816bca18 127.0.0.1:1031            127.0.0.1:1032            664
0x814ab950 10.0.2.15:1369            10.0.124.198:445          1272
0x8152f720 10.0.2.15:1376            10.0.194.216:445          1272
0x814f46a0 10.0.2.15:1343            10.0.4.225:445            1272
0x814f5300 10.0.2.15:1366            10.0.73.206:445           1272
0x8134dc60 10.0.2.15:1363            10.0.22.213:445           1272
0x8151fcd8 10.0.2.15:1390            10.0.90.11:445            1272
0x8166c370 10.0.2.15:1360            10.0.227.220:445          1272
0x814f6e68 10.0.2.15:1387            10.0.39.19:445            1272
0x814c4938 10.0.2.15:1357            10.0.176.100:445          1272
0x8137a4e8 10.0.2.15:1384            10.0.244.25:445           1272
0x815d0830 10.0.2.15:1351            10.0.54.162:445           1272
0x81533a58 10.0.2.15:1374            10.0.123.15:445           1272
0x81637258 10.0.2.15:1354            10.0.125.107:445          1272
0x814ce528 10.0.2.15:1348            10.0.3.170:445            1272
0x8151e2f0 10.0.2.15:1381            10.0.194.161:445          1272
0x814fde68 10.0.2.15:1371            10.0.72.23:445            1272
0x816cdca0 10.0.2.15:1378            10.0.143.168:445          1272
0x815e0008 10.0.2.15:1345            10.0.208.177:445          1272
0x815308c0 10.0.2.15:1368            10.0.21.158:445           1272
0x81631e68 10.0.2.15:1342            10.0.158.184:445          1272
0x81525630 10.0.2.15:1365            10.0.226.165:445          1272
0x81690b40 10.0.2.15:1362            10.0.176.173:445          1272
0x814dccd8 10.0.2.15:1389            10.0.244.226:445          1272
0x815e4b40 10.0.2.15:1359            10.0.125.180:445          1272
0x81530cc8 10.0.2.15:1105            10.0.254.7:445            1492
0x814fc630 10.0.2.15:1386            10.0.193.234:445          1272
0x81507b28 10.0.2.15:1145            10.0.2.34:445             1492
0x814b08b8 10.0.2.15:1356            10.0.74.188:445           1272
0x81534e68 10.0.2.15:1383            10.0.142.241:445          1272
0x815046d0 10.0.2.15:1350            10.0.208.250:445          1272
0x8150e8c0 10.0.2.15:1373            10.0.21.231:445           1272
0x8153acf0 10.0.2.15:1353            10.0.23.196:445           1272
0x814ee438 10.0.2.15:1380            10.0.91.249:445           1272
0x81342e68 10.0.2.15:1347            10.0.157.1:445            1272
0x81374e08 10.0.2.15:1370            10.0.226.238:445          1272
0x81631620 10.0.2.15:1377            10.0.41.129:445           1272
0x81529008 10.0.2.15:1344            10.0.106.137:445          1272
0x81691850 10.0.2.15:1340            10.0.107.192:445          1272
0x813547b0 10.0.2.15:1367            10.0.175.246:445          1272
0x814f6280 10.0.2.15:1341            10.0.55.145:445           1272
0x815e1488 10.0.2.15:1364            10.0.124.253:445          1272
0x814ec718 10.0.2.15:1074            10.0.0.163:445            0
0x816cde40 10.0.2.15:1098            10.0.1.20:445             1492
```

4- **Where are the remote IP addresses/domain name located?**

As seen in the previous section, it makes communication via all the local addresses. (in our analyzed system as 10.0.*.*)

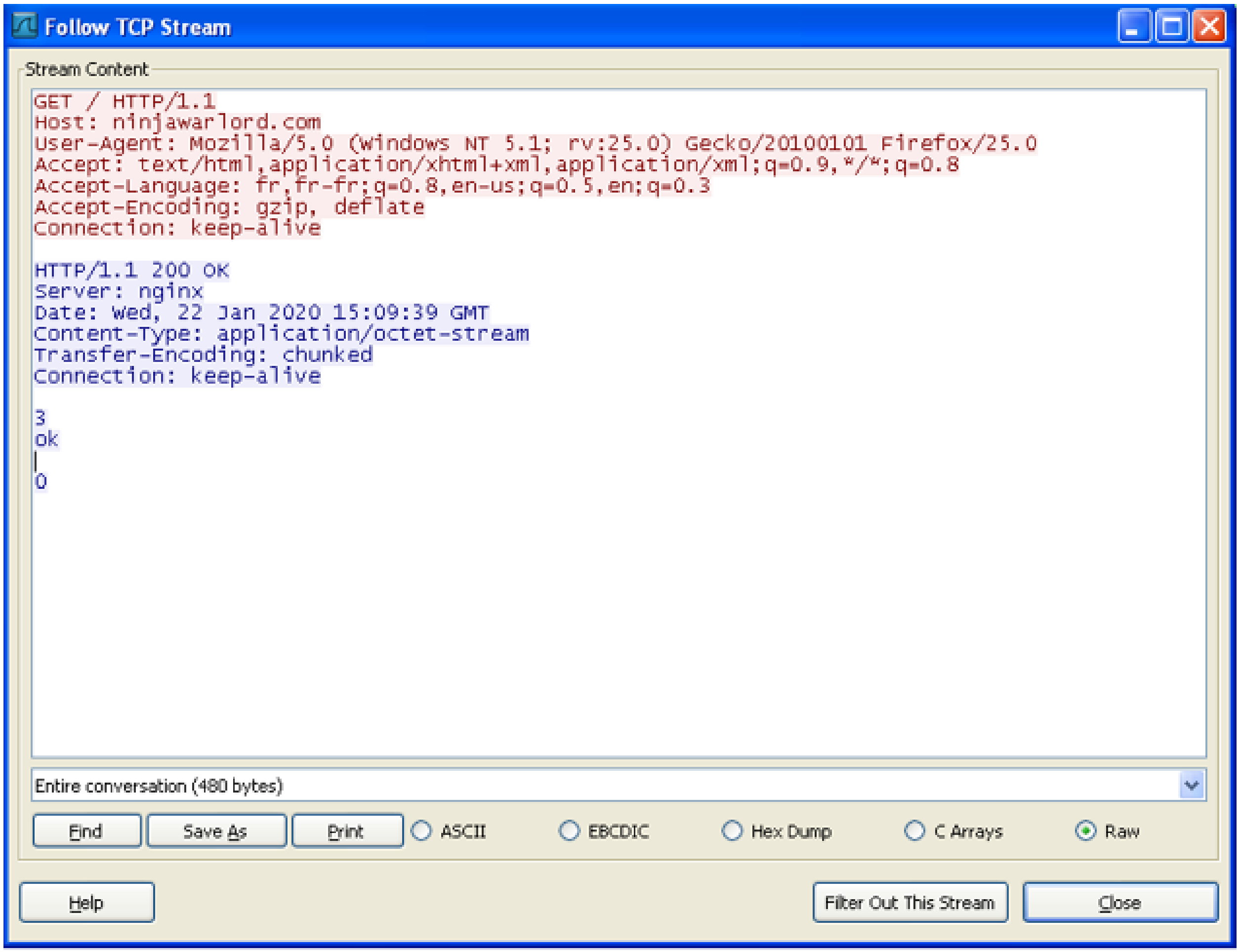
Also, by using the packet tracer, we found that 172.20.10.1 / ninjawarlord.com are making the communication remotely.



AMD PCNET Family Ethernet Adapter (Microsoft's Packet Scheduler) : \Device\NPF_{47F0A2FA-6DF1-4964-96F4-4A387234992C} [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
22	0.54279600	10.0.2.15	10.0.88.254	TCP	62	4245 > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
23	1.71418400	10.0.2.15	172.20.10.1	DNS	76	Standard query 0x11eb A ninjawarlord.com
24	1.72022400	172.20.10.1	10.0.2.15	DNS	92	Standard query response 0x11eb A 35.187.36.248
25	1.72077900	10.0.2.15	35.187.36.248	TCP	62	4246 > worldscores [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
26	2.05284500	10.0.2.15	10.0.35.38	TCP	62	4196 > microsoft-ds [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1



```
GET / HTTP/1.1
Host: ninjawarlord.com
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:25.0) Gecko/20100101 Firefox/25.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 22 Jan 2020 15:09:39 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: keep-alive

3
ok

0
```

Entire conversation (480 bytes)

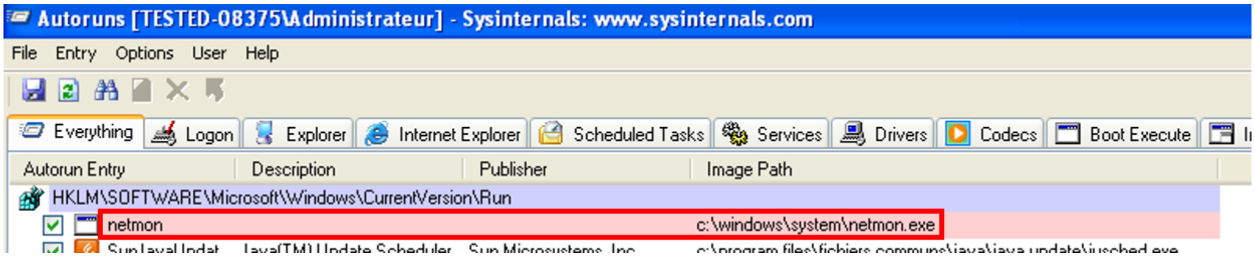
○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Also, we investigated the site Ninjaworld.com, where it downloads some remote files from this website.

5- Find where the malicious program is recorded in the registry startup list

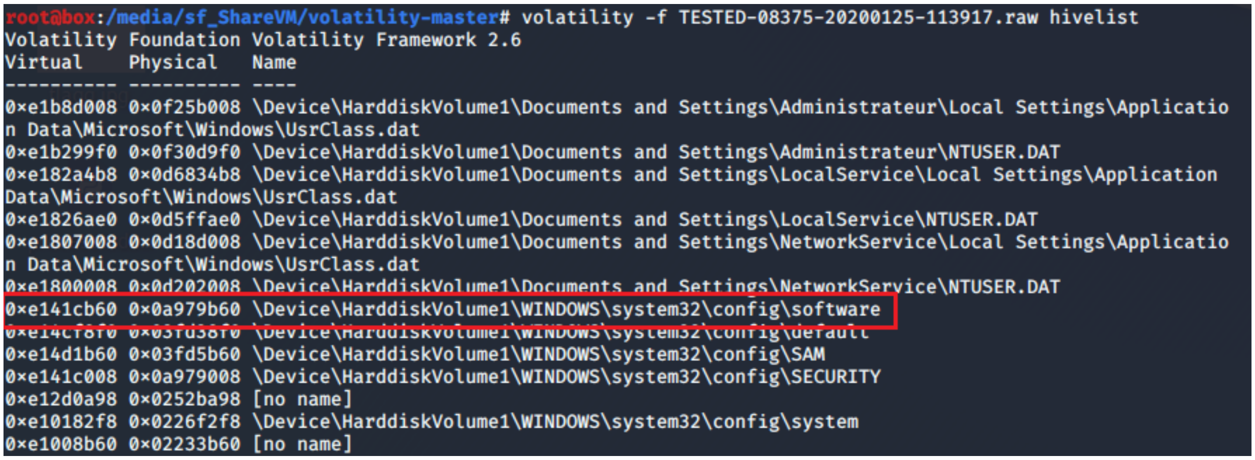
By using the Autoruns file, we have found the Registry startup file location of the malicious program netmon.

The file is under →**HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**



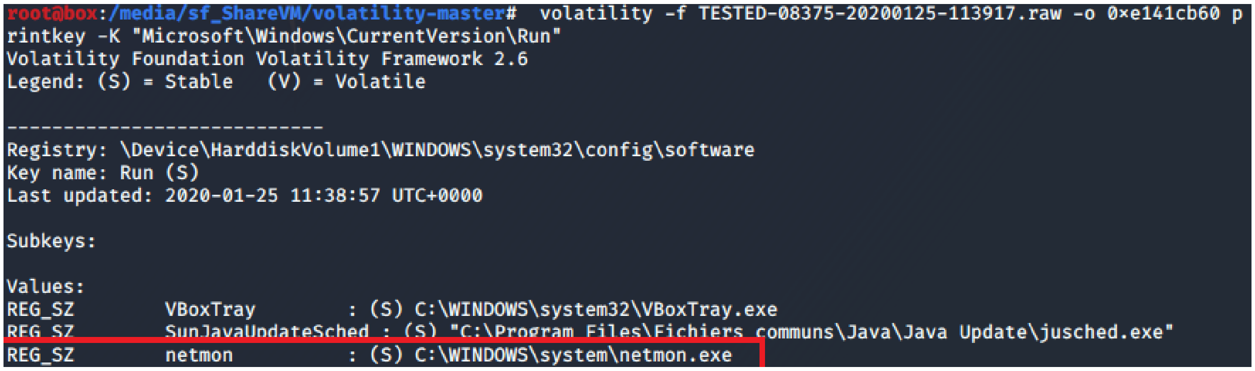
Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ netmon			c:\windows\system\netmon.exe
☑ SunJavaUpdat	Java(TM) Update Scheduler	Sun Microsystems, Inc.	c:\program files\fichiers communs\java\java update\jusched.exe

Also using the volatility, we found the hive list an using the key found the below process



```
root@box:/media/sf_ShareVM/volatility-master# volatility -f TESTED-08375-20200125-113917.raw hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0×e1b8d008 0×0f25b008 \Device\HarddiskVolume1\Documents and Settings\Administrateur\Local Settings\Applicatio
n Data\Microsoft\Windows\UsrClass.dat
0×e1b299f0 0×0f30d9f0 \Device\HarddiskVolume1\Documents and Settings\Administrateur\NTUSER.DAT
0×e182a4b8 0×0d6834b8 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application
Data\Microsoft\Windows\UsrClass.dat
0×e1826ae0 0×0d5ffae0 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0×e1807008 0×0d18d008 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Applicatio
n Data\Microsoft\Windows\UsrClass.dat
0×e1800008 0×0d202008 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0×e141cb60 0×0a979b60 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0×e14cf8f0 0×03fd38f0 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0×e14d1b60 0×03fd5b60 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0×e141c008 0×0a979008 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0×e12d0a98 0×0252ba98 [no name]
0×e10182f8 0×0226f2f8 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0×e1008b60 0×02233b60 [no name]
```

Screenshot to showing the Hive list



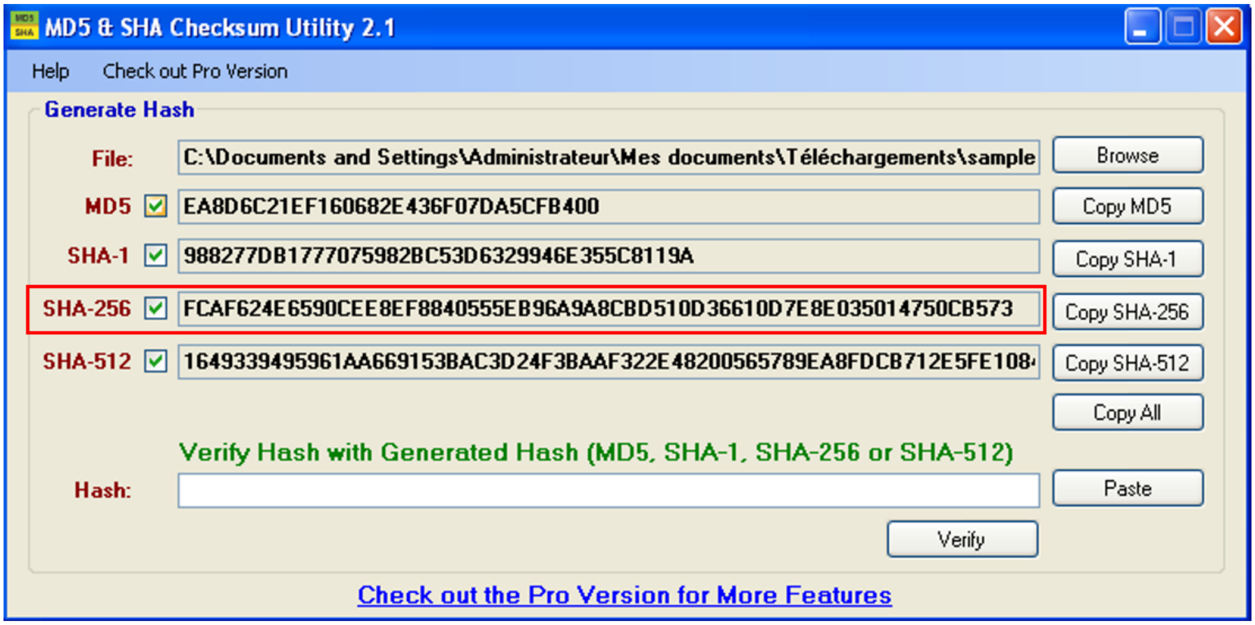
```
root@box:/media/sf_ShareVM/volatility-master#  volatility -f TESTED-08375-20200125-113917.raw -o 0×e141cb60 p
rintkey -K "Microsoft\Windows\CurrentVersion\Run"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: Run (S)
Last updated: 2020-01-25 11:38:57 UTC+0000

Subkeys:

Values:
REG_SZ        VBoxTray            : (S) C:\WINDOWS\system32\VBoxTray.exe
REG_SZ        SunJavaUpdateSched  : (S) "C:\Program Files\Fichiers communs\Java\Java Update\jusched.exe"
REG_SZ        netmon              : (S) C:\WINDOWS\system\netmon.exe
```

Screenshot to showing the sub process keys

We just analyzed using the volatility hive list and it displayed us a registry list and acquired the offset of **\WINDOWS\system32\config\software** and key as **Microsft\Windows\CurrentVersion\Run**.

- ➔ netmon is exist in **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**

6- What's the SHA256 of this malware?



Generate Hash

File: C:\Documents and Settings\Administrateur\Mes documents\Téléchargements\sample

MD5 ☑ EA8D6C21EF160682E436F07DA5CFB400

SHA-1 ☑ 988277DB1777075982BC53D6329946E355C8119A

SHA-256 ☑ FCAF624E6590CEE8EF8840555EB96A9A8CBD510D36610D7E8E035014750CB573

SHA-512 ☑ 1649339495961AA669153BAC3D24F3BAAF322E48200565789EA8FDCB712E5FE108

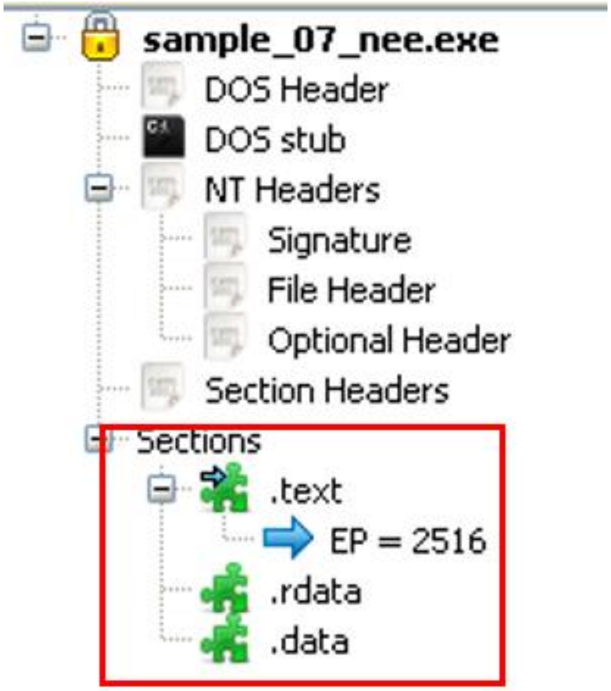
Verify Hash with Generated Hash (MD5, SHA-1, SHA-256 or SHA-512)

Hash:

7- What are the sections of this PE file?

During our memory Forensics analysis, we found that

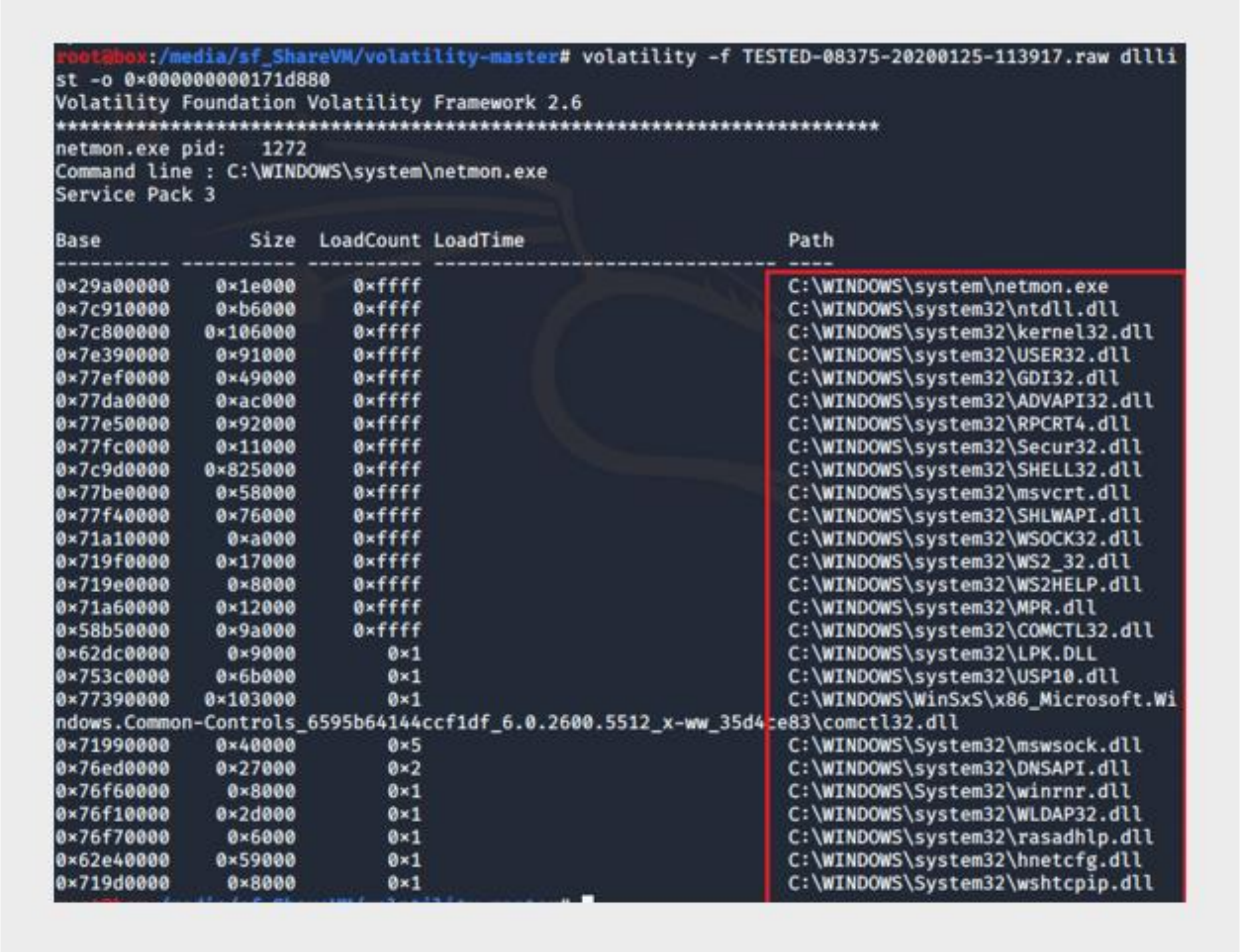
→. text,. rdata, and .data are the sections under the PE file.



```
sample_07_nee.exe
    DOS Header
    DOS stub
    NT Headers
        Signature
        File Header
        Optional Header
    Section Headers
    Sections
        .text
            EP = 2516
        .rdata
        .data
```

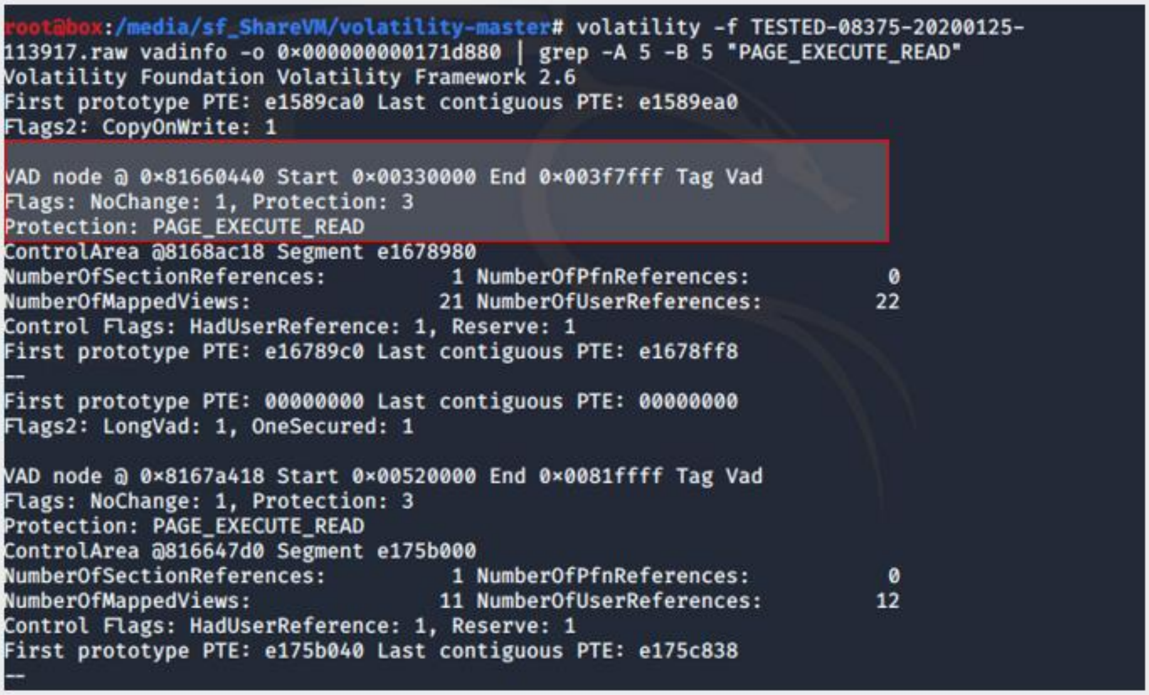
8. How does this malware executes its code on the system? dump it.

Analyzing the .dll files using the .dll utility of volatility - the corresponding .dll to netmon offset and others seems to be legitimate.



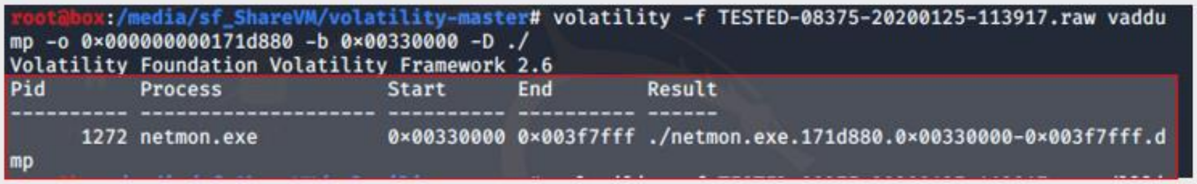
```
root@box:/media/sf_ShareVM/volatility-master# volatility -f TESTED-08375-20200125-113917.raw dllli
st -o 0x000000000171d880
Volatility Foundation Volatility Framework 2.6
************************************************************************
netmon.exe pid:   1272
Command line : C:\WINDOWS\system\netmon.exe
Service Pack 3

Base             Size  LoadCount LoadTime                       Path
---------- ---------- ---------- ------------------------------ ----
0x29a00000    0x1e000     0xffff                                C:\WINDOWS\system\netmon.exe
0x7c910000    0xb6000     0xffff                                C:\WINDOWS\system32\ntdll.dll
0x7c800000   0x106000     0xffff                                C:\WINDOWS\system32\kernel32.dll
0x7e390000    0x91000     0xffff                                C:\WINDOWS\system32\USER32.dll
0x77ef0000    0x49000     0xffff                                C:\WINDOWS\system32\GDI32.dll
0x77da0000    0xac000     0xffff                                C:\WINDOWS\system32\ADVAPI32.dll
0x77e50000    0x92000     0xffff                                C:\WINDOWS\system32\RPCRT4.dll
0x77fc0000    0x11000     0xffff                                C:\WINDOWS\system32\Secur32.dll
0x7c9d0000   0x825000     0xffff                                C:\WINDOWS\system32\SHELL32.dll
0x77be0000    0x58000     0xffff                                C:\WINDOWS\system32\msvcrt.dll
0x77f40000    0x76000     0xffff                                C:\WINDOWS\system32\SHLWAPI.dll
0x71a10000     0xa000     0xffff                                C:\WINDOWS\system32\WSOCK32.dll
0x719f0000    0x17000     0xffff                                C:\WINDOWS\system32\WS2_32.dll
0x719e0000     0x8000     0xffff                                C:\WINDOWS\system32\WS2HELP.dll
0x71a60000    0x12000     0xffff                                C:\WINDOWS\system32\MPR.dll
0x58b50000    0x9a000     0xffff                                C:\WINDOWS\system32\COMCTL32.dll
0x62dc0000     0x9000        0x1                                C:\WINDOWS\system32\LPK.DLL
0x753c0000    0x6b000        0x1                                C:\WINDOWS\system32\USP10.dll
0x77390000   0x103000        0x1                                C:\WINDOWS\WinSxS\x86_Microsoft.Wi
ndows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
0x71990000    0x40000        0x5                                C:\WINDOWS\System32\mswsock.dll
0x76ed0000    0x27000        0x2                                C:\WINDOWS\system32\DNSAPI.dll
0x76f60000     0x8000        0x1                                C:\WINDOWS\System32\winrnr.dll
0x76f10000    0x2d000        0x1                                C:\WINDOWS\system32\WLDAP32.dll
0x76f70000     0x6000        0x1                                C:\WINDOWS\system32\rasadhlp.dll
0x62e40000    0x59000        0x1                                C:\WINDOWS\system32\hnetcfg.dll
0x719d0000     0x8000        0x1                                C:\WINDOWS\System32\wshtcpip.dll
```

Also, we have checked the PAGE_EXECUTE_READ permissions without creating the file on disk and we found the matching memory block .



```
root@box:/media/sf_ShareVM/volatility-master# volatility -f TESTED-08375-20200125-
113917.raw vadinfo -o 0x000000000171d880 | grep -A 5 -B 5 "PAGE_EXECUTE_READ"
Volatility Foundation Volatility Framework 2.6
First prototype PTE: e1589ca0 Last contiguous PTE: e1589ea0
Flags2: CopyOnWrite: 1

VAD node @ 0x81660440 Start 0x00330000 End 0x003f7fff Tag Vad
Flags: NoChange: 1, Protection: 3
Protection: PAGE_EXECUTE_READ
ControlArea @8168ac18 Segment e1678980
NumberOfSectionReferences:          1 NumberOfPfnReferences:           0
NumberOfMappedViews:               21 NumberOfUserReferences:         22
Control Flags: HadUserReference: 1, Reserve: 1
First prototype PTE: e16789c0 Last contiguous PTE: e1678ff8
--
First prototype PTE: 00000000 Last contiguous PTE: 00000000
Flags2: LongVad: 1, OneSecured: 1

VAD node @ 0x8167a418 Start 0x00520000 End 0x0081ffff Tag Vad
Flags: NoChange: 1, Protection: 3
Protection: PAGE_EXECUTE_READ
ControlArea @816647d0 Segment e175b000
NumberOfSectionReferences:          1 NumberOfPfnReferences:           0
NumberOfMappedViews:               11 NumberOfUserReferences:         12
Control Flags: HadUserReference: 1, Reserve: 1
First prototype PTE: e175b040 Last contiguous PTE: e175c838
--
```

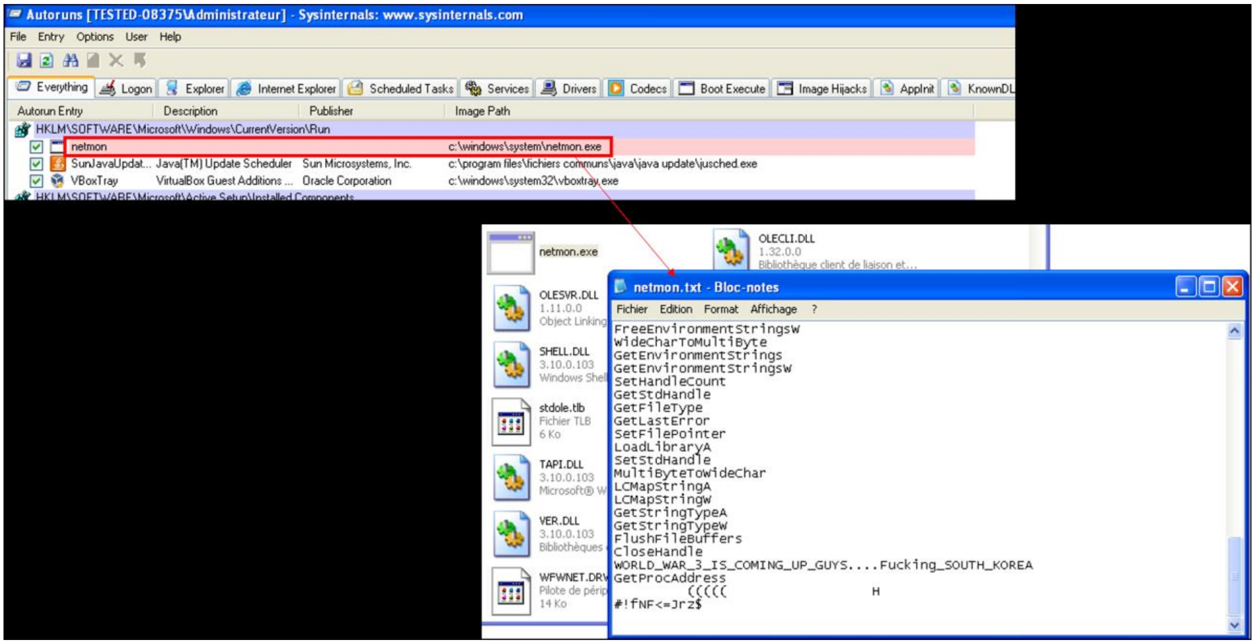
By using the utility of the vaddump, we can see the memory page with start index **0x00330000** corresponding to netmon



```
root@box:/media/sf_ShareVM/volatility-master# volatility -f TESTED-08375-20200125-113917.raw vaddu
mp -o 0x000000000171d880 -b 0x00330000 -D ./
Volatility Foundation Volatility Framework 2.6
Pid        Process              Start      End        Result
---------- -------------------- ---------- ---------- ------
      1272 netmon.exe           0x00330000 0x003f7fff ./netmon.exe.171d880.0x00330000-0x003f7fff.d
mp
```

9- What is this malware's name?

→The malware name is ***netmon.exe.***



Autoruns [TESTED-08375\Administrateur] - Sysinternals: www.sysinternals.com

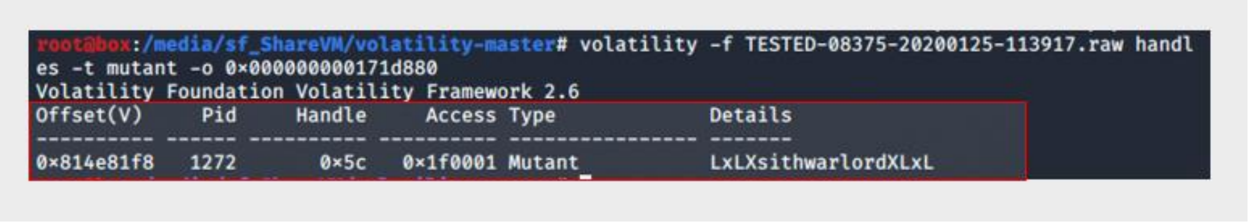
Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ netmon			c:\windows\system\netmon.exe
☑ SunJavaUpdat...	Java(TM) Update Scheduler	Sun Microsystems, Inc.	c:\program files\fichiers communs\java\java update\jusched.exe
☑ VBoxTray	VirtualBox Guest Additions ...	Oracle Corporation	c:\windows\system32\vboxtray.exe
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			

netmon.txt - Bloc-notes

```
FreeEnvironmentStringsW
WideCharToMultiByte
GetEnvironmentStrings
GetEnvironmentStringsW
SetHandleCount
GetStdHandle
GetFileType
GetLastError
SetFilePointer
LoadLibraryA
SetStdHandle
MultiByteToWideChar
LCMapStringA
LCMapStringW
GetStringTypeA
GetStringTypeW
FlushFileBuffers
CloseHandle
WORLD_WAR_3_IS_COMING_UP_GUYS....Fucking_SOUTH_KOREA
GetProcAddress
          (((((                 H
#!fNF<=Jrz$
```

11- Give its mutexes.

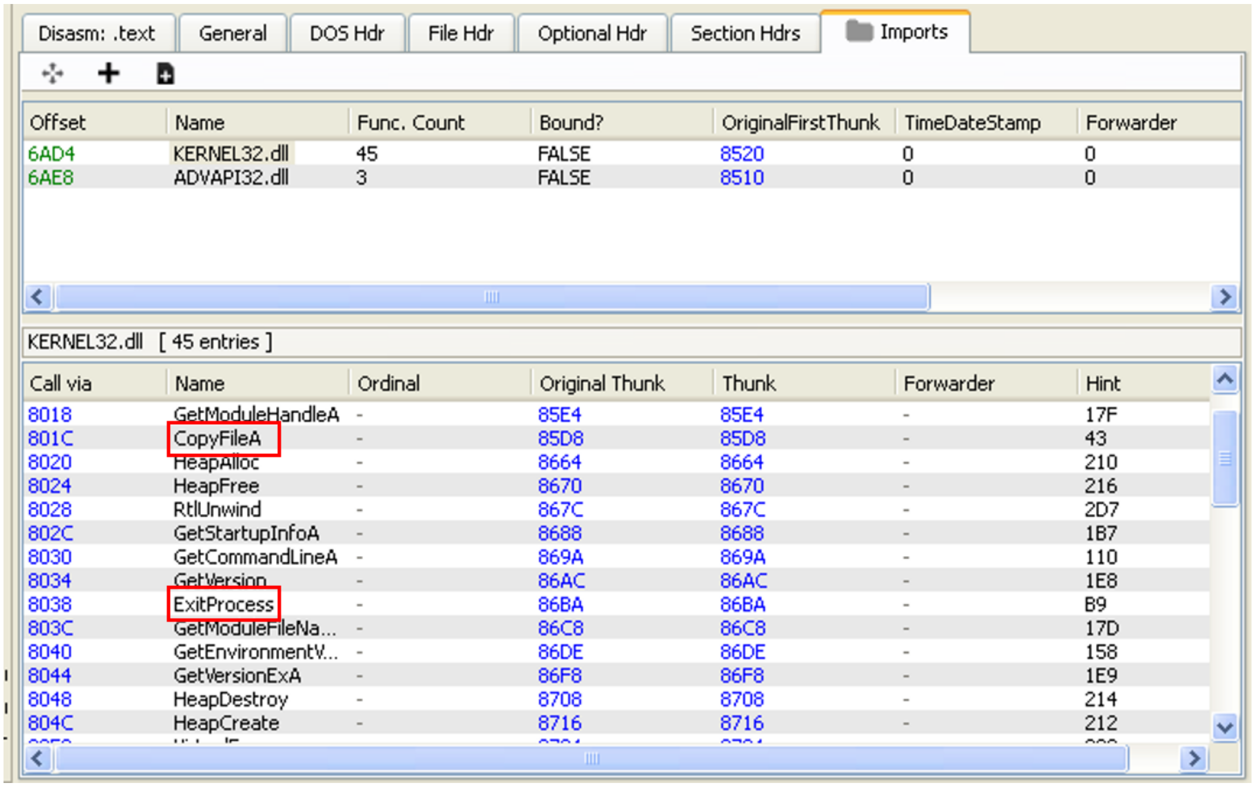
We found the handes and mutants' utility of the Volatility tool and found the corresponding mutexes as **LxLXsithwarlordXLxL**



```
root@box:/media/sf_ShareVM/volatility-master# volatility -f TESTED-08375-20200125-113917.raw handl
es -t mutant -o 0×000000000171d880
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid      Handle      Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0×814e81f8    1272        0×5c    0×1f0001 Mutant           LxLXsithwarlordXLxL
```

12- What are the hooked API? From which processes?

We suspect that the below CopyFileaA Exitprocess are the hooked API



Offset	Name	Func. Count	Bound?	OriginalFirstThunk	TimeDateStamp	Forwarder
6AD4	KERNEL32.dll	45	FALSE	8520	0	0
6AE8	ADVAPI32.dll	3	FALSE	8510	0	0

KERNEL32.dll [45 entries]

Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
8018	GetModuleHandleA	-	85E4	85E4	-	17F
801C	CopyFileA	-	85D8	85D8	-	43
8020	HeapAlloc	-	8664	8664	-	210
8024	HeapFree	-	8670	8670	-	216
8028	RtlUnwind	-	867C	867C	-	2D7
802C	GetStartupInfoA	-	8688	8688	-	1B7
8030	GetCommandLineA	-	869A	869A	-	110
8034	GetVersion	-	86AC	86AC	-	1E8
8038	ExitProcess	-	86BA	86BA	-	B9
803C	GetModuleFileNa...	-	86C8	86C8	-	17D
8040	GetEnvironmentV...	-	86DE	86DE	-	158
8044	GetVersionExA	-	86F8	86F8	-	1E9
8048	HeapDestroy	-	8708	8708	-	214
804C	HeapCreate	-	8716	8716	-	212

Also,we tried in volatality to find the apihooks, but there is no other API which comes under .netmon offsets

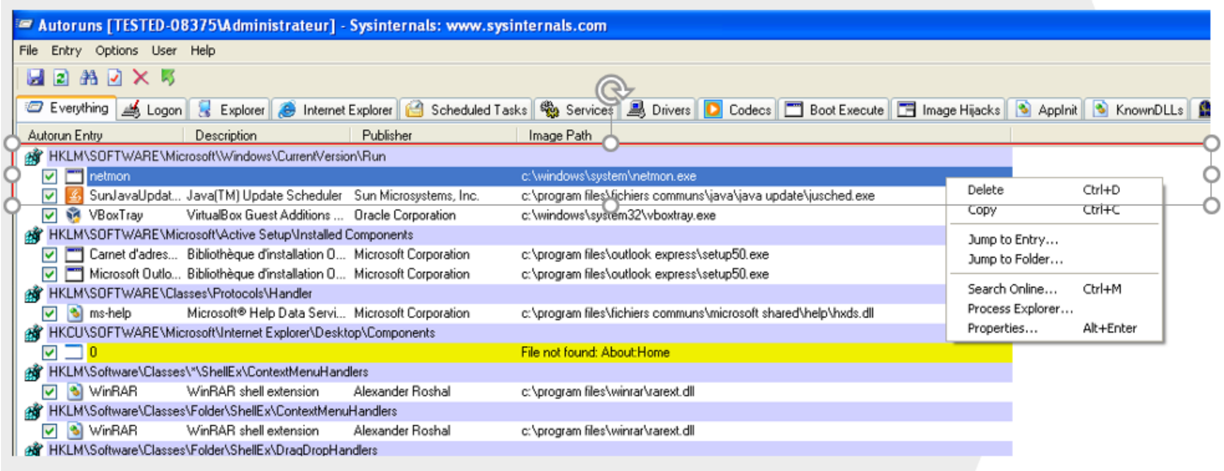
13- Does this malware propagate/spread itself?

Yes, as already discussed the malware propagates via port 445.

DISINFECTION

Write a script/program to clean an infected system automatically. If you can’t do it, show the manual steps.

Manual Steps:



Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ netmon			c:\windows\system\netmon.exe
☑ SunJavaUpdat...	Java(TM) Update Scheduler	Sun Microsystems, Inc.	c:\program files\fichiers communs\java\java update\jusched.exe
☑ VBoxTray	VirtualBox Guest Additions ...	Oracle Corporation	c:\windows\system32\vboxtray.exe
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			
☑ Carnet d'adres...	Bibliothèque d'installation O...	Microsoft Corporation	c:\program files\outlook express\setup50.exe
☑ Microsoft Outlo...	Bibliothèque d'installation O...	Microsoft Corporation	c:\program files\outlook express\setup50.exe
HKLM\SOFTWARE\Classes\Protocols\Handler			
☑ ms-help	Microsoft® Help Data Servi...	Microsoft Corporation	c:\program files\fichiers communs\microsoft shared\help\hxds.dll
HKCU\SOFTWARE\Microsoft\Internet Explorer\Desktop\Components			
☑ 0			File not found: About:Home
HKLM\Software\Classes\*\ShellEx\ContextMenuHandlers			
☑ WinRAR	WinRAR shell extension	Alexander Roshal	c:\program files\winrar\rarext.dll
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers			
☑ WinRAR	WinRAR shell extension	Alexander Roshal	c:\program files\winrar\rarext.dll
HKLM\Software\Classes\Folder\ShellEx\DragDropHandlers			

- ➔ We deleted the entry from the registry.
- ➔ We have restarted my system after deleting the entry from key registry.
- ➔ We were able to delete the malware.

We also confirmed by examining the Wireshark and there is no malware communication via netmon and 445 port.

Automation of disinfection:

Also, we tried a script to delete the infection file and auto restart to recover state.

```
import os
os.remove("C:₩WINDOWS₩system₩netmon.exe")
print("File Removed!")
print "REBOOTING"
os.system("shutdown -t 0 -r -f")
```