MALWARE ANALYSIS REPORT

Report by: Yogitha Satya Sai Pantham

Jad

Sneha

INDEX

SUMMARY

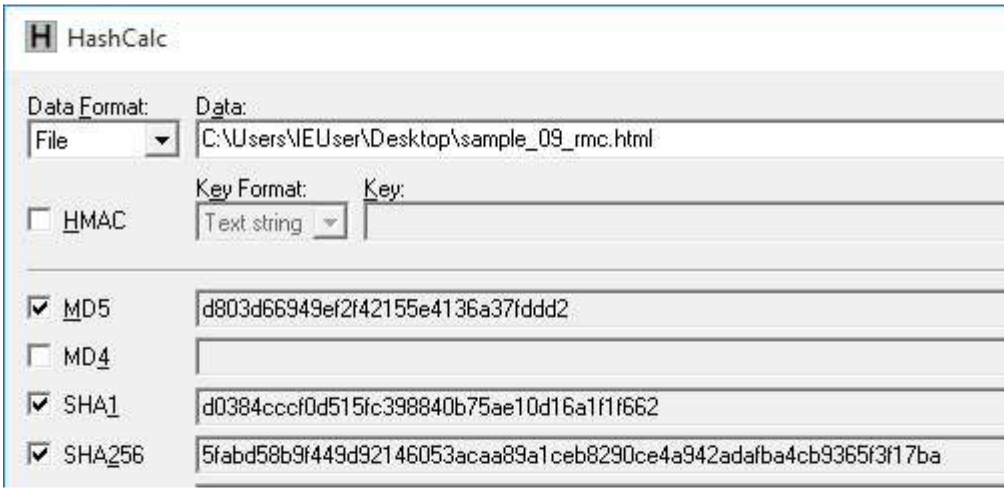
DESCRIPTION:

Malware also known as malicious software , is a program developed for the purpose of harming a computer, without the concern of the user. This report shows, behaviour of this malware “Sample_09_rmc.html” in computer by doingmalware analysis.

IDENTIFICATION:

We can identify malware by

1. SHA256



HashCalc

Data Format: File

Data: C:\Users\IEUser\Desktop\sample_09_rmc.html

□ HMAC Key Format: Text string Key:

☑ MD5 d803d66949ef2f42155e4136a37fddd2

□ MD4

☑ SHA1 d0384cccf0d515fc398840b75ae10d16a1f1f662

☑ SHA256 5fabd58b9f449d92146053acaa89a1ceb8290ce4a942adafba4cb9365f3f17ba

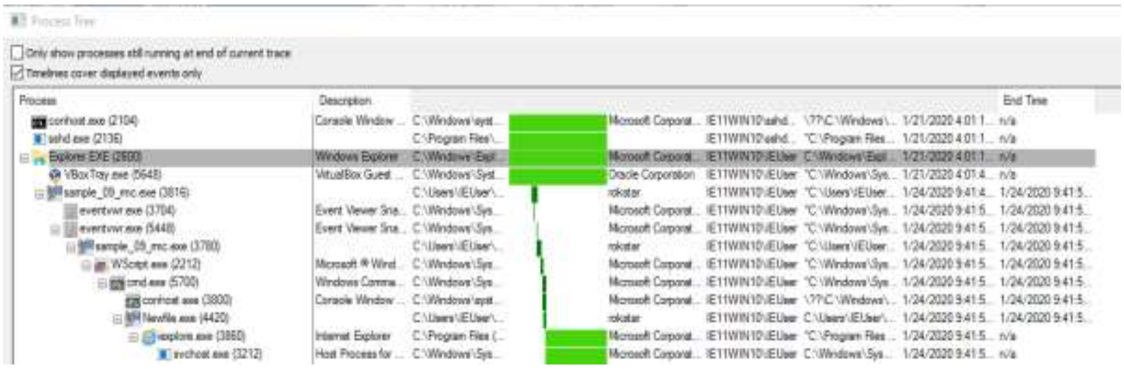
2. FILE

3. STRINGS

4. CFF EXPLORER.

DYNAMIC ANALYSIS: This is performed Using digital forensics tools:

1. PROCMON

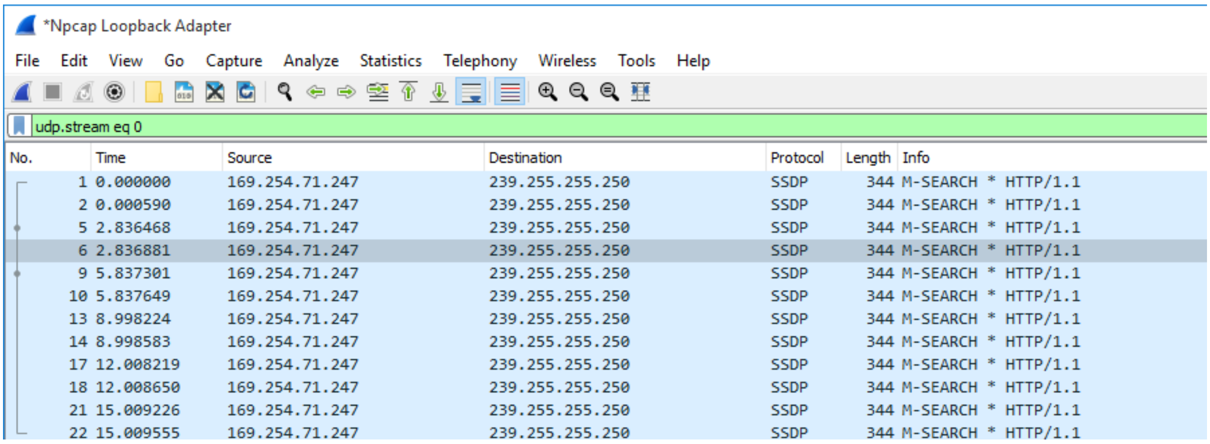


Process Tree

☐ Only show processes still running at end of current trace
☑ Timelines cover displayed events only

Process	Description						End Time
conhost.exe (2104)	Console Window ...	C:\Windows\syst...	Microsoft Corporat...	IE11WIN10\sshd...	\??\C:\Windows\...	1/21/2020 4:01:1...	n/a
sshd.exe (2136)		C:\Program Files\...		IE11WIN10\sshd...	"C:\Program Files...	1/21/2020 4:01:1...	n/a
Explorer.EXE (2600)	Windows Explorer	C:\Windows\Expl...	Microsoft Corporat...	IE11WIN10\IEUser	C:\Windows\Expl...	1/21/2020 4:01:1...	n/a
VBoxTray.exe (5648)	VirtualBox Guest ...	C:\Windows\Syst...	Oracle Corporation	IE11WIN10\IEUser	"C:\Windows\Sys...	1/21/2020 4:01:4...	n/a
sample_09_mc.exe (3816)		C:\Users\IEUser\...	rokstar	IE11WIN10\IEUser	"C:\Users\IEUser...	1/24/2020 9:41:4...	1/24/2020 9:41:5...
eventvwr.exe (3704)	Event Viewer Sna...	C:\Windows\Sys...	Microsoft Corporat...	IE11WIN10\IEUser	"C:\Windows\Sys...	1/24/2020 9:41:5...	1/24/2020 9:41:5...
eventvwr.exe (5448)	Event Viewer Sna...	C:\Windows\Sys...	Microsoft Corporat...	IE11WIN10\IEUser	"C:\Windows\Sys...	1/24/2020 9:41:5...	1/24/2020 9:41:5...
sample_09_mc.exe (3780)		C:\Users\IEUser\...	rokstar	IE11WIN10\IEUser	"C:\Users\IEUser...	1/24/2020 9:41:5...	1/24/2020 9:41:5...
WScript.exe (2212)	Microsoft ® Wind...	C:\Windows\Sys...	Microsoft Corporat...	IE11WIN10\IEUser	"C:\Windows\Sys...	1/24/2020 9:41:5...	1/24/2020 9:41:5...
cmd.exe (5700)	Windows Comma...	C:\Windows\Sys...	Microsoft Corporat...	IE11WIN10\IEUser	"C:\Windows\Sys...	1/24/2020 9:41:5...	1/24/2020 9:41:5...
conhost.exe (3800)	Console Window ...	C:\Windows\syst...	Microsoft Corporat...	IE11WIN10\IEUser	\??\C:\Windows\...	1/24/2020 9:41:5...	1/24/2020 9:41:5...
Newfile.exe (4420)		C:\Users\IEUser\...	rokstar	IE11WIN10\IEUser	C:\Users\IEUser\...	1/24/2020 9:41:5...	1/24/2020 9:41:5...
iexplore.exe (3860)	Internet Explorer	C:\Program Files (...	Microsoft Corporat...	IE11WIN10\IEUser	"C:\Program Files...	1/24/2020 9:41:5...	n/a
svchost.exe (3212)	Host Process for ...	C:\Windows\Sys...	Microsoft Corporat...	IE11WIN10\IEUser	C:\Windows\Sys...	1/24/2020 9:41:5...	n/a

2. TCP VIEW

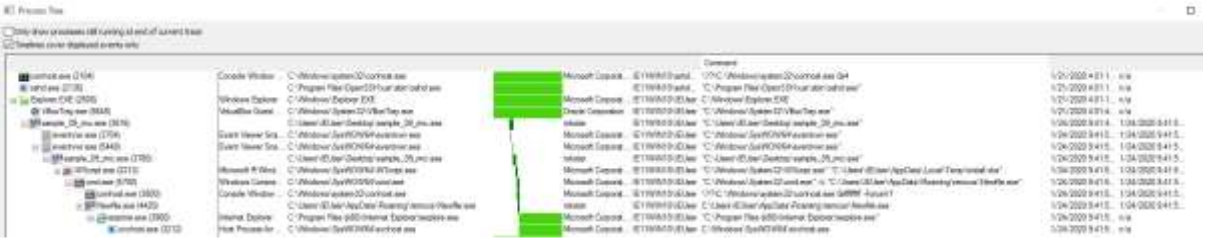


*Npcap Loopback Adapter

udp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	169.254.71.247	239.255.255.250	SSDP	344	M-SEARCH * HTTP/1.1
2	0.000590	169.254.71.247	239.255.255.250	SSDP	344	M-SEARCH * HTTP/1.1
5	2.836468	169.254.71.247	239.255.255.250	SSDP	344	M-SEARCH * HTTP/1.1
6	2.836881	169.254.71.247	239.255.255.250	SSDP	344	M-SEARCH * HTTP/1.1
9	5.837301	169.254.71.247	239.255.255.250	SSDP	344	M-SEARCH * HTTP/1.1
10	5.837649	169.254.71.247	239.255.255.250	SSDP	344	M-SEARCH * HTTP/1.1
13	8.998224	169.254.71.247	239.255.255.250	SSDP	344	M-SEARCH * HTTP/1.1
14	8.998583	169.254.71.247	239.255.255.250	SSDP	344	M-SEARCH * HTTP/1.1
17	12.008219	169.254.71.247	239.255.255.250	SSDP	344	M-SEARCH * HTTP/1.1
18	12.008650	169.254.71.247	239.255.255.250	SSDP	344	M-SEARCH * HTTP/1.1
21	15.009226	169.254.71.247	239.255.255.250	SSDP	344	M-SEARCH * HTTP/1.1
22	15.009555	169.254.71.247	239.255.255.250	SSDP	344	M-SEARCH * HTTP/1.1

3. AUTORUN



Process Tree

☐ Only show processes still running at end of current trace
☑ Timelines cover displayed events only

					Command		
conhost.exe (2104)	Console Window ...	C:\Windows\system32\conhost.exe	Microsoft Corporat...	IE11WIN10\sshd...	\??\C:\Windows\system32\conhost.exe 0x4	1/21/2020 4:01:1...	n/a
sshd.exe (2136)		C:\Program Files\OpenSSH\usr\sbin\sshd.exe		IE11WIN10\sshd...	"C:\Program Files\OpenSSH\usr\sbin\sshd.exe"	1/21/2020 4:01:1...	n/a
Explorer.EXE (2600)	Windows Explorer	C:\Windows\Explorer.EXE	Microsoft Corporat...	IE11WIN10\IEUser	C:\Windows\Explorer.EXE	1/21/2020 4:01:1...	n/a
VBoxTray.exe (5648)	VirtualBox Guest ...	C:\Windows\System32\VBoxTray.exe	Oracle Corporation	IE11WIN10\IEUser	"C:\Windows\System32\VBoxTray.exe"	1/21/2020 4:01:4...	n/a
sample_09_mc.exe (3816)		C:\Users\IEUser\Desktop\sample_09_mc.exe	rokstar	IE11WIN10\IEUser	"C:\Users\IEUser\Desktop\sample_09_mc.exe"	1/24/2020 9:41:4...	1/24/2020 9:41:5...
eventvwr.exe (3704)	Event Viewer Sna...	C:\Windows\SysWOW64\eventvwr.exe	Microsoft Corporat...	IE11WIN10\IEUser	"C:\Windows\SysWOW64\eventvwr.exe"	1/24/2020 9:41:5...	1/24/2020 9:41:5...
eventvwr.exe (5448)	Event Viewer Sna...	C:\Windows\SysWOW64\eventvwr.exe	Microsoft Corporat...	IE11WIN10\IEUser	"C:\Windows\SysWOW64\eventvwr.exe"	1/24/2020 9:41:5...	1/24/2020 9:41:5...
sample_09_mc.exe (3780)		C:\Users\IEUser\Desktop\sample_09_mc.exe	rokstar	IE11WIN10\IEUser	"C:\Users\IEUser\Desktop\sample_09_mc.exe"	1/24/2020 9:41:5...	1/24/2020 9:41:5...
WScript.exe (2212)	Microsoft ® Wind...	C:\Windows\SysWOW64\WScript.exe	Microsoft Corporat...	IE11WIN10\IEUser	"C:\Windows\System32\WScript.exe" "C:\Users\IEUser\AppData\Local\Temp\install.vbs"	1/24/2020 9:41:5...	1/24/2020 9:41:5...
cmd.exe (5700)	Windows Comma...	C:\Windows\SysWOW64\cmd.exe	Microsoft Corporat...	IE11WIN10\IEUser	"C:\Windows\System32\cmd.exe" /c "C:\Users\IEUser\AppData\Roaming\[illegible]\Newfile.exe"	1/24/2020 9:41:5...	1/24/2020 9:41:5...
conhost.exe (3800)	Console Window ...	C:\Windows\system32\conhost.exe	Microsoft Corporat...	IE11WIN10\IEUser	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	1/24/2020 9:41:5...	1/24/2020 9:41:5...
Newfile.exe (4420)		C:\Users\IEUser\AppData\Roaming\[illegible]\Newfile.exe	rokstar	IE11WIN10\IEUser	C:\Users\IEUser\AppData\Roaming\[illegible]\Newfile.exe	1/24/2020 9:41:5...	1/24/2020 9:41:5...
iexplore.exe (3860)	Internet Explorer	C:\Program Files (x86)\Internet Explorer\iexplore.exe	Microsoft Corporat...	IE11WIN10\IEUser	"C:\Program Files (x86)\Internet Explorer\iexplore.exe"	1/24/2020 9:41:5...	n/a
svchost.exe (3212)	Host Process for ...	C:\Windows\SysWOW64\svchost.exe	Microsoft Corporat...	IE11WIN10\IEUser	C:\Windows\SysWOW64\svchost.exe	1/24/2020 9:41:5...	n/a

4.Memory dump generation

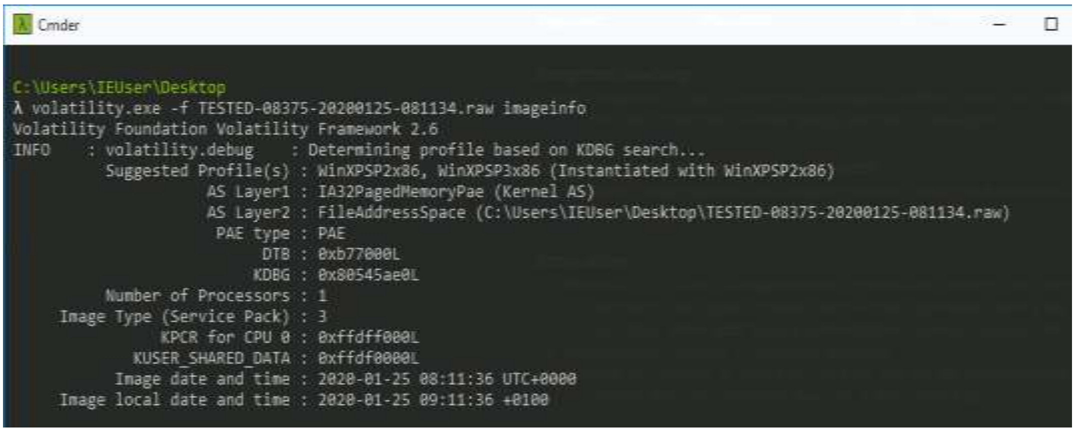
S.NO	Memory analysis Q & A
1	From which operating system's version this image was taken?
2	What are the strange processes? Are they malicious? Why?
3	Which process is making network connections?
4	Where are the remote IP addresses/domain name located?
5	Find where the malicious program is recorded in the registry startup list
6	What's the SHA256 of this malware?
7	What are the sections of this PE file?
8	Any interesting strings from this malware?
9	How does this malware executes its code on the system? dump it.
10	What is this malware's name?
11	Give its mutexes
12	What are the hooked API? From which processes?
13	Does this malware propagate/spread itself?

14	Write a script/program to clean an infected system automatically. If you aren't able to do it, show the manual steps

Q & A

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

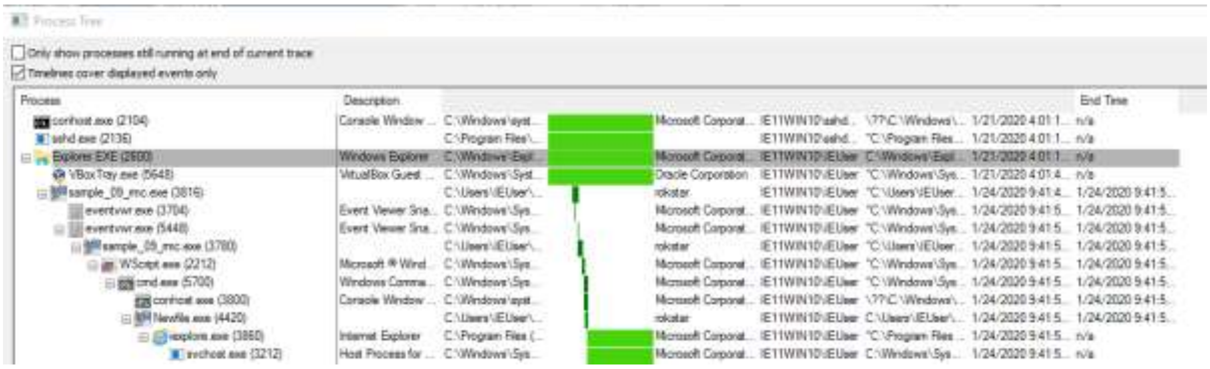
The image was taken from WinXPSP2x86, WinXPSP3x86 as shown below.



```
C:\Users\IEUser\Desktop
λ volatility.exe -f TESTED-08375-20200125-081134.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\IEUser\Desktop\TESTED-08375-20200125-081134.raw)
                      PAE type : PAE
                           DTB : 0xb77000L
                          KDBG : 0x80545ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2020-01-25 08:11:36 UTC+0000
     Image local date and time : 2020-01-25 09:11:36 +0100
```

2. What are the strange processes? Are they malicious? Why?

The strange processes are newfile.exe and cmd exe



□ Only show processes still running at end of current trace

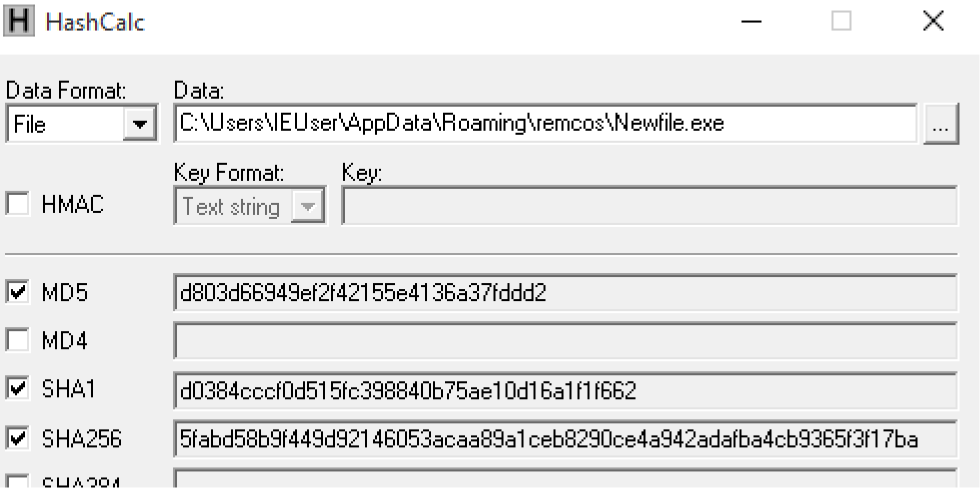
☑ Timelines cover displayed events only

Process	Description							End Time
conhost.exe (2104)	Console Window ...	C:\Windows\syst...	🟩	Microsoft Corporat...	IE11WIN10\sshd...	\??\C:\Windows\...	1/21/2020 4:01:1...	n/a
sshd.exe (2136)		C:\Program Files\...	🟩		IE11WIN10\sshd...	"C:\Program Files...	1/21/2020 4:01:1...	n/a
Explorer.EXE (2600)	Windows Explorer	C:\Windows\Expl...	🟩	Microsoft Corporat...	IE11WIN10\IEUser	C:\Windows\Expl...	1/21/2020 4:01:1...	n/a
VBoxTray.exe (5648)	VirtualBox Guest ...	C:\Windows\Syst...	🟩	Oracle Corporation	IE11WIN10\IEUser	"C:\Windows\Sys...	1/21/2020 4:01:4...	n/a
sample_09_mc.exe (3816)		C:\Users\IEUser\...		rokstar	IE11WIN10\IEUser	"C:\Users\IEUser...	1/24/2020 9:41:4...	1/24/2020 9:41:5...
eventvwr.exe (3704)	Event Viewer Sna...	C:\Windows\Sys...		Microsoft Corporat...	IE11WIN10\IEUser	"C:\Windows\Sys...	1/24/2020 9:41:5...	1/24/2020 9:41:5...
eventvwr.exe (5448)	Event Viewer Sna...	C:\Windows\Sys...		Microsoft Corporat...	IE11WIN10\IEUser	"C:\Windows\Sys...	1/24/2020 9:41:5...	1/24/2020 9:41:5...
sample_09_mc.exe (3780)		C:\Users\IEUser\...		rokstar	IE11WIN10\IEUser	"C:\Users\IEUser...	1/24/2020 9:41:5...	1/24/2020 9:41:5...
WScript.exe (2212)	Microsoft ® Wind...	C:\Windows\Sys...		Microsoft Corporat...	IE11WIN10\IEUser	"C:\Windows\Sys...	1/24/2020 9:41:5...	1/24/2020 9:41:5...
cmd.exe (5700)	Windows Comma...	C:\Windows\Sys...		Microsoft Corporat...	IE11WIN10\IEUser	"C:\Windows\Sys...	1/24/2020 9:41:5...	1/24/2020 9:41:5...
conhost.exe (3800)	Console Window ...	C:\Windows\syst...		Microsoft Corporat...	IE11WIN10\IEUser	\??\C:\Windows\...	1/24/2020 9:41:5...	1/24/2020 9:41:5...
Newfile.exe (4420)		C:\Users\IEUser\...		rokstar	IE11WIN10\IEUser	C:\Users\IEUser\...	1/24/2020 9:41:5...	1/24/2020 9:41:5...
iexplore.exe (3860)	Internet Explorer	C:\Program Files (...	🟩	Microsoft Corporat...	IE11WIN10\IEUser	"C:\Program Files ...	1/24/2020 9:41:5...	n/a
svchost.exe (3212)	Host Process for ...	C:\Windows\Sys...	🟩	Microsoft Corporat...	IE11WIN10\IEUser	C:\Windows\Sys...	1/24/2020 9:41:5...	n/a

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

4. **Where are the remote IP addresses/domain name located?**
5. **Find where the malicious program is recorded in the registry startup list**
6. **What's the SHA256 of this malware?**

The SHA256 of this malware is 5fabd58b9f449d92146053acaa89a1ceb8290ce4a942adafb9365f3f17ba



HashCalc

Data Format: File

Data: C:\Users\IEUser\AppData\Roaming\remcos\Newfile.exe

□ HMAC Key Format: Text string Key:

☑ MD5 d803d66949ef2f42155e4136a37fddd2

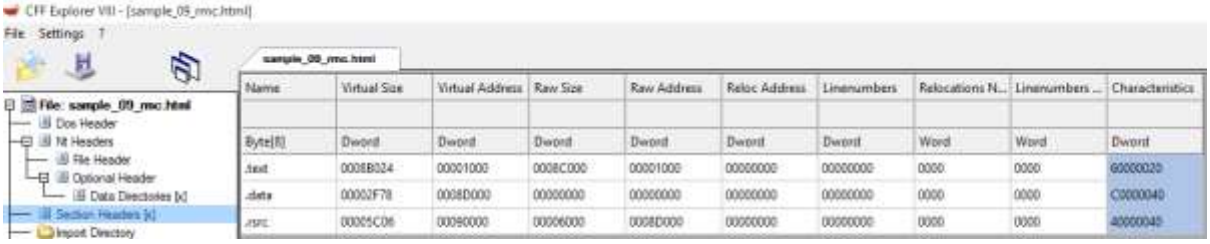
□ MD4

☑ SHA1 d0384cccf0d515fc398840b75ae10d16a1f1f662

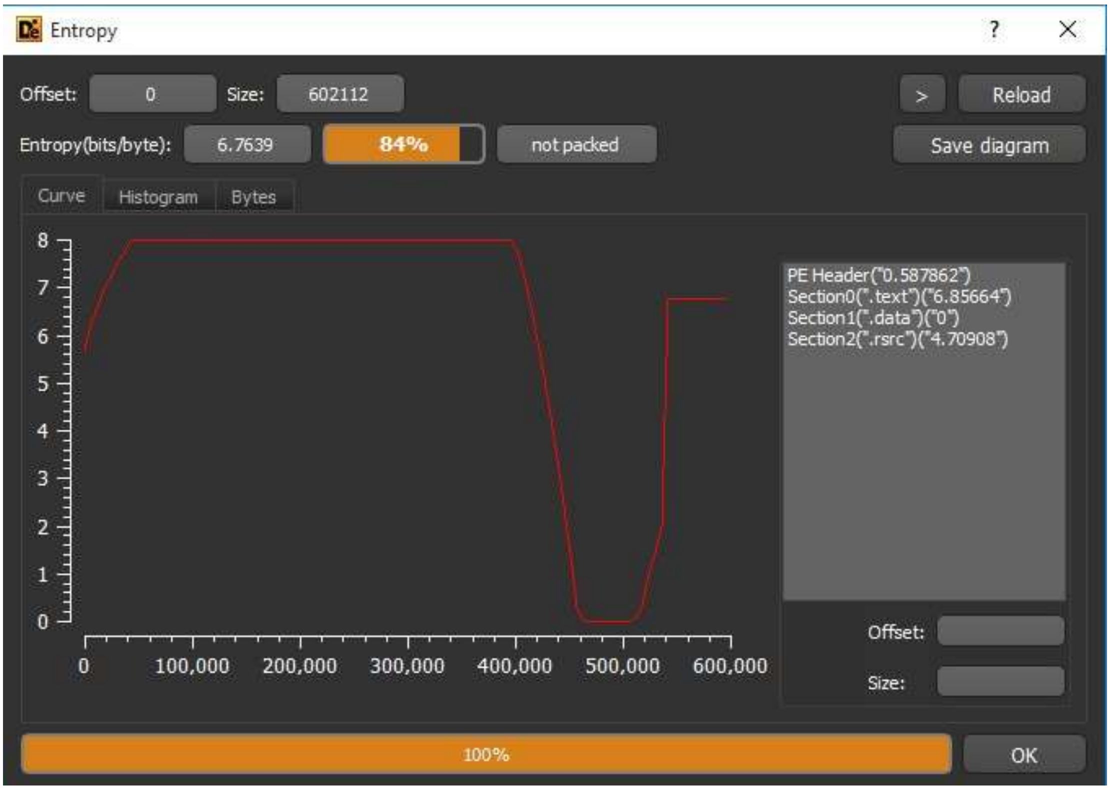
☑ SHA256 5fabd58b9f449d92146053acaa89a1ceb8290ce4a942adafba4cb9365f3f17ba

□ SHA384

7. What are the sections of this PE file?



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	0008B024	00001000	0008C000	00001000	00000000	00000000	0000	0000	60000020
.data	00002F78	0008D000	00000000	00000000	00000000	00000000	0000	0000	C0000040
.rsrc	00005C06	00090000	00006000	0008D000	00000000	00000000	0000	0000	40000040



Offset: 0 Size: 602112

Entropy(bits/byte): 6.7639 84% not packed

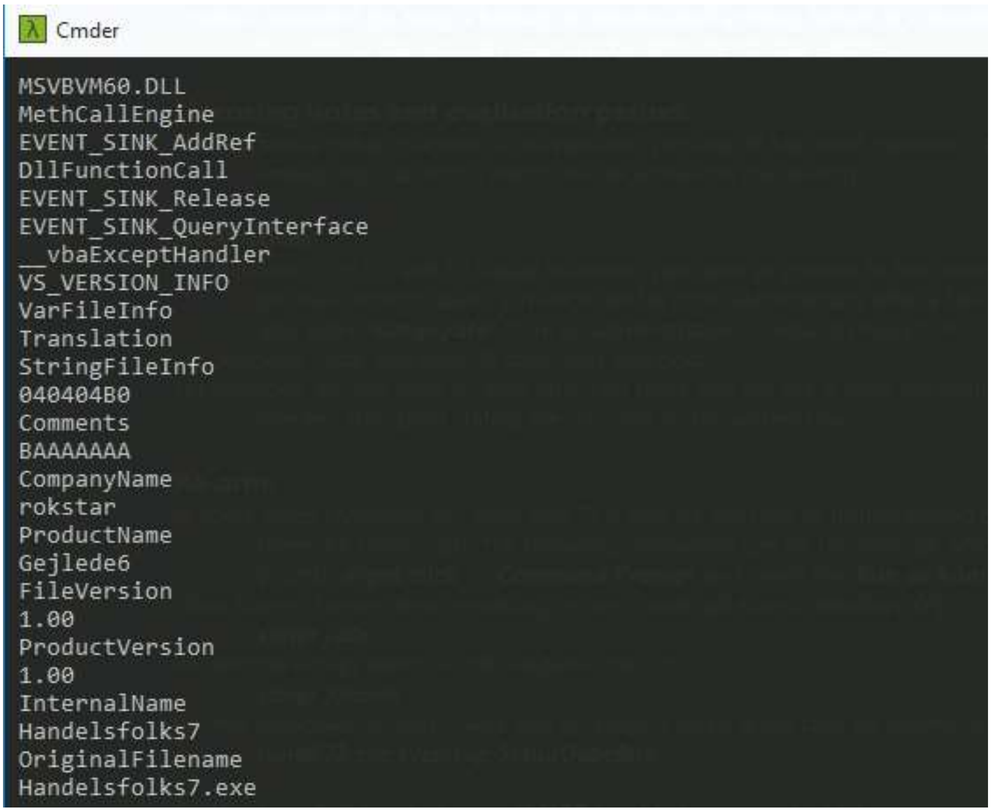
PE Header("0.587862")
Section0(".text")("6.85664")
Section1(".data")("0")
Section2(".rsrc")("4.70908")

Offset:

Size:

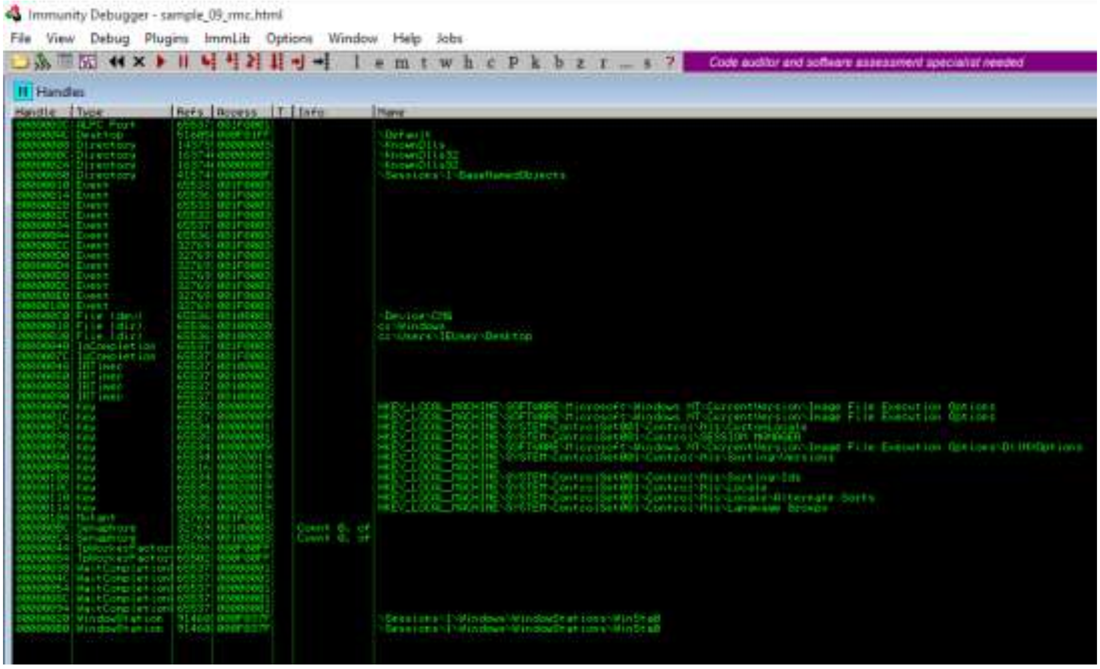
100%

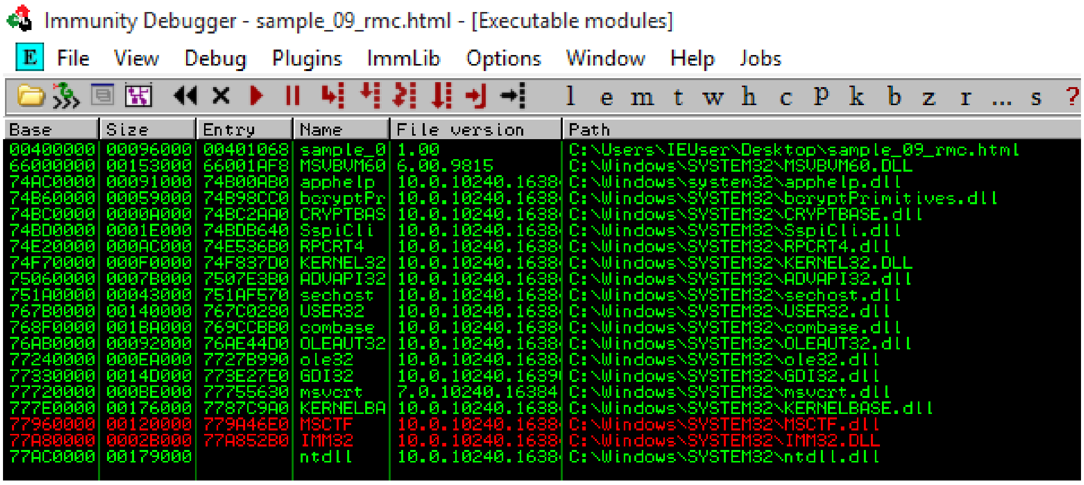
8. Any interesting strings from this malware?



```
MSVBVM60.DLL
MethCallEngine
EVENT_SINK_AddRef
DllFunctionCall
EVENT_SINK_Release
EVENT_SINK_QueryInterface
__vbaExceptHandler
VS_VERSION_INFO
VarFileInfo
Translation
StringFileInfo
040404B0
Comments
BAAAAAAA
CompanyName
rokstar
ProductName
Gejlede6
FileVersion
1.00
ProductVersion
1.00
InternalName
Handelsfolks7
OriginalFilename
Handelsfolks7.exe
```

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

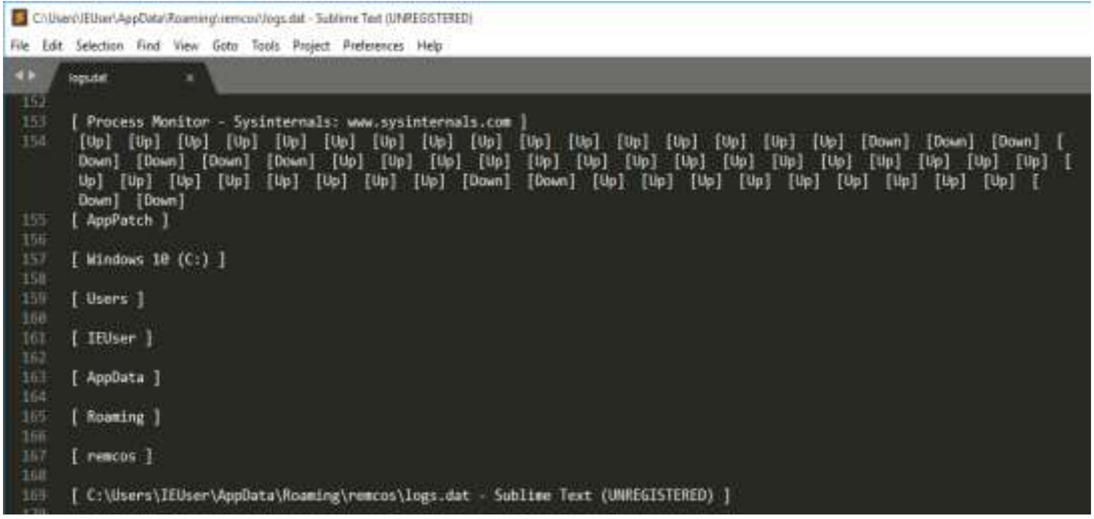

Immunity Debugger - sample_09_rmc.html
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Code auditor and software assessment specialist needed
Handles
Handle Type Refs Access T Info Name


Immunity Debugger - sample_09_rmc.html - [Executable modules]
E File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?

```
Base     Size     Entry    Name     File version    Path
00400000 00096000 00401068 sample_0 1.00            C:\Users\IEUser\Desktop\sample_09_rmc.html
66000000 00153000 66001AF8 MSVBVM60 6.00.9815       C:\Windows\SYSTEM32\MSVBVM60.DLL
74AC0000 00091000 74B00AB0 apphelp  10.0.10240.1638 C:\Windows\system32\apphelp.dll
74B60000 00059000 74B98CC0 bcryptPr 10.0.10240.1638 C:\Windows\SYSTEM32\bcryptPrimitives.dll
74BC0000 0000A000 74BC2AA0 CRYPTBAS 10.0.10240.1638 C:\Windows\SYSTEM32\CRYPTBASE.dll
74BD0000 0001E000 74BDB640 SspiCli  10.0.10240.1638 C:\Windows\SYSTEM32\SspiCli.dll
74E20000 000AC000 74E536B0 RPCRT4   10.0.10240.1638 C:\Windows\SYSTEM32\RPCRT4.dll
74F70000 000F0000 74F837D0 KERNEL32 10.0.10240.1638 C:\Windows\SYSTEM32\KERNEL32.DLL
75060000 0007B000 7507E3B0 ADVAPI32 10.0.10240.1638 C:\Windows\SYSTEM32\ADVAPI32.dll
751A0000 00043000 751AF570 sechost  10.0.10240.1638 C:\Windows\SYSTEM32\sechost.dll
767B0000 00140000 767C0280 USER32   10.0.10240.1638 C:\Windows\SYSTEM32\USER32.dll
768F0000 001BA000 769CCBB0 combase  10.0.10240.1638 C:\Windows\SYSTEM32\combase.dll
76AB0000 00092000 76AE44D0 OLEAUT32 10.0.10240.1638 C:\Windows\SYSTEM32\OLEAUT32.dll
77240000 000EA000 7727B990 ole32    10.0.10240.1638 C:\Windows\SYSTEM32\ole32.dll
77330000 0014D000 773E27E0 GDI32    10.0.10240.1639 C:\Windows\SYSTEM32\GDI32.dll
77720000 000BE000 77755630 msvcrt   7.0.10240.16384 C:\Windows\SYSTEM32\msvcrt.dll
777E0000 00176000 7787C9A0 KERNELBA 10.0.10240.1638 C:\Windows\SYSTEM32\KERNELBASE.dll
77960000 00120000 779A46E0 MSCTF    10.0.10240.1638 C:\Windows\SYSTEM32\MSCTF.dll
77A80000 0002B000 77A852B0 IMM32    10.0.10240.1638 C:\Windows\SYSTEM32\IMM32.DLL
77AC0000 00179000          ntdll    10.0.10240.1638 C:\Windows\SYSTEM32\ntdll.dll
```

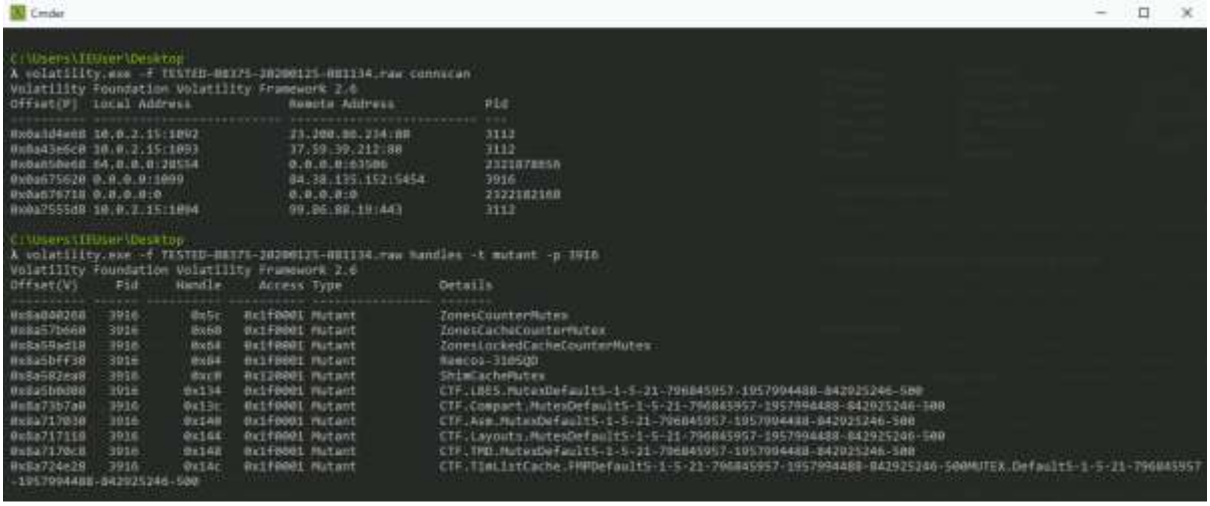
10. What is this malware's name?

The malware is a Keylogger.


C:\Users\IEUser\AppData\Roaming\remcos\logs.dat - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
logs.dat

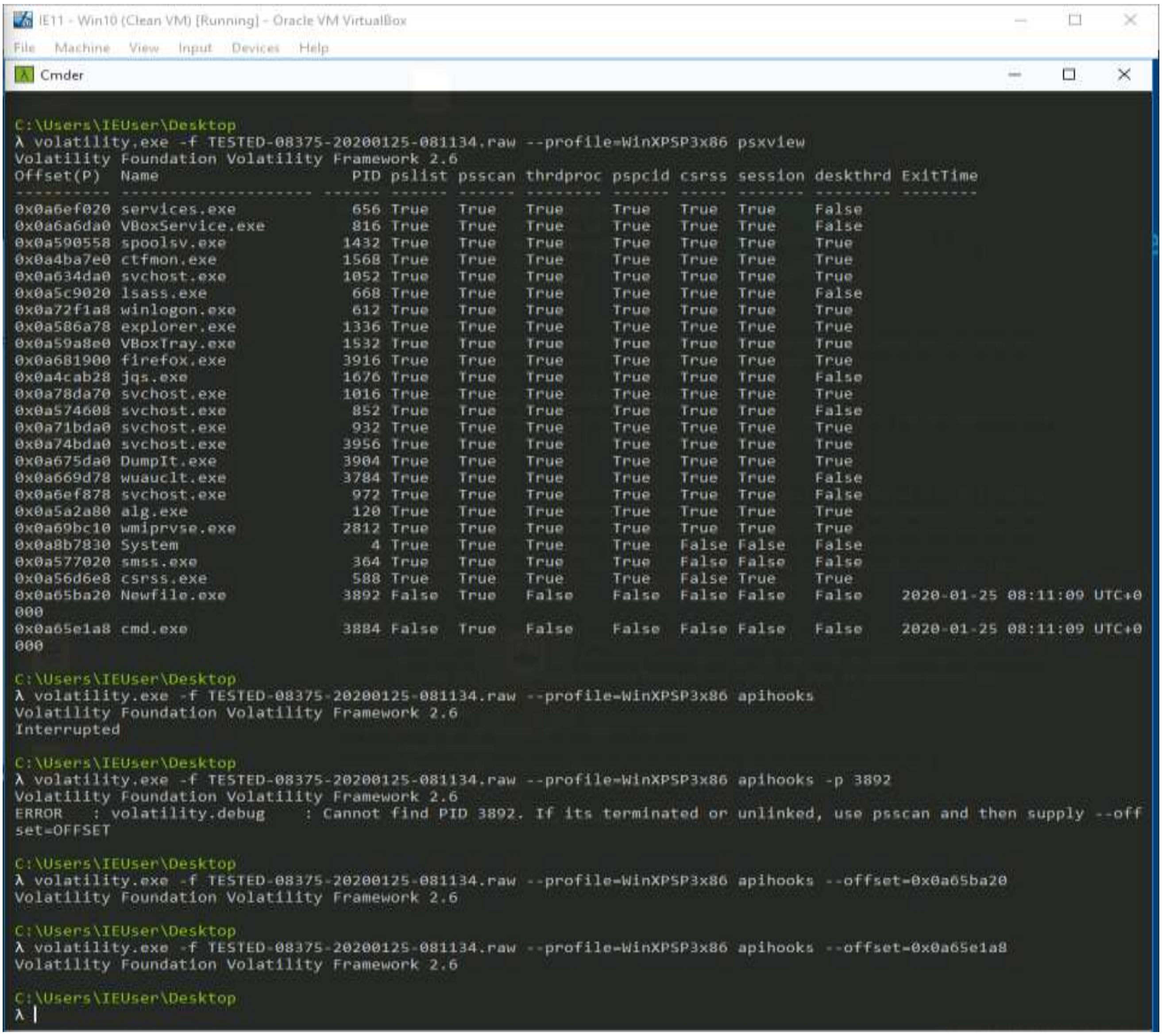
```

[ Process Monitor - Sysinternals: www.sysinternals.com ]
 [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Down] [Down] [Down] [
 Down] [Down] [Down] [Down] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [
 Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Down] [Down] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [
 Down] [Down]
[ AppPatch ]

[ Windows 10 (C:) ]

[ Users ]

[ IEUser ]

[ AppData ]

[ Roaming ]

[ remcos ]

[ C:\Users\IEUser\AppData\Roaming\remcos\logs.dat - Sublime Text (UNREGISTERED) ]
```

11. Give its mutexes.



```
C:\Users\IEUser\Desktop
λ volatility.exe -f TESTED-88375-20200125-081134.raw connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x0a3d4e08 10.0.2.15:1092            23.200.86.234:80          3112
0x0a43e6c0 10.0.2.15:1093            37.59.39.212:80           3112
0x0a050e68 64.0.0.0:28554            0.0.0.0:63500             2321878856
0x0a675620 0.0.0.0:1099              84.38.135.152:5454        3916
0x0a676718 0.0.0.0:0                 0.0.0.0:0                 2322182160
0x0a2555d8 10.0.2.15:1094            99.86.88.18:443           3112

C:\Users\IEUser\Desktop
λ volatility.exe -f TESTED-88375-20200125-081134.raw handles -t mutant -p 3916
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid      Handle     Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0x8a040268   3916       0x5c   0x1f0001 Mutant           ZonesCounterMutex
0x8a57b660   3916       0x60   0x1f0001 Mutant           ZonesCacheCounterMutex
0x8a59ad18   3916       0x64   0x1f0001 Mutant           ZonesLockedCacheCounterMutex
0x8a5bff38   3916       0x84   0x1f0001 Mutant           Remcos-310SQD
0x8a582ea8   3916       0xc0   0x120001 Mutant           ShimCacheMutex
0x8a5b0d08   3916      0x134   0x1f0001 Mutant           CTF.LBES.MutexDefaultS-1-5-21-796845957-1957994488-842925246-500
0x8a73b7a0   3916      0x13c   0x1f0001 Mutant           CTF.Compart.MutexDefaultS-1-5-21-796845957-1957994488-842925246-500
0x8a717030   3916      0x140   0x1f0001 Mutant           CTF.Asm.MutexDefaultS-1-5-21-796845957-1957994488-842925246-500
0x8a717110   3916      0x144   0x1f0001 Mutant           CTF.Layouts.MutexDefaultS-1-5-21-796845957-1957994488-842925246-500
0x8a7170c8   3916      0x148   0x1f0001 Mutant           CTF.TMD.MutexDefaultS-1-5-21-796845957-1957994488-842925246-500
0x8a724e28   3916      0x14c   0x1f0001 Mutant           CTF.TimListCache.FMPDefaultS-1-5-21-796845957-1957994488-842925246-500MUTEX.DefaultS-1-5-21-796845957
-1957994488-842925246-500
```

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



IE11 - Win10 (Clean VM) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Cmder

```
C:\Users\IEUser\Desktop
λ volatility.exe -f TESTED-08375-20200125-081134.raw --profile=WinXPSP3x86 psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x0a6ef020 services.exe            656 True   True   True     True   True  True    False
0x0a6a6da0 VBoxService.exe         816 True   True   True     True   True  True    False
0x0a590558 spoolsv.exe            1432 True   True   True     True   True  True    True
0x0a4ba7e0 ctfmon.exe             1568 True   True   True     True   True  True    True
0x0a634da0 svchost.exe            1052 True   True   True     True   True  True    True
0x0a5c9020 lsass.exe               668 True   True   True     True   True  True    False
0x0a72f1a8 winlogon.exe            612 True   True   True     True   True  True    True
0x0a586a78 explorer.exe           1336 True   True   True     True   True  True    True
0x0a59a8e0 VBoxTray.exe           1532 True   True   True     True   True  True    True
0x0a681900 firefox.exe            3916 True   True   True     True   True  True    True
0x0a4cab28 jqs.exe                1676 True   True   True     True   True  True    False
0x0a78da70 svchost.exe            1016 True   True   True     True   True  True    True
0x0a574608 svchost.exe             852 True   True   True     True   True  True    False
0x0a71bda0 svchost.exe             932 True   True   True     True   True  True    True
0x0a74bda0 svchost.exe            3956 True   True   True     True   True  True    True
0x0a675da0 DumpIt.exe             3904 True   True   True     True   True  True    True
0x0a669d78 wuauclt.exe            3784 True   True   True     True   True  True    False
0x0a6ef878 svchost.exe             972 True   True   True     True   True  True    False
0x0a5a2a80 alg.exe                 120 True   True   True     True   True  True    True
0x0a69bc10 wmiprvse.exe           2812 True   True   True     True   True  True    True
0x0a8b7830 System                    4 True   True   True     True   False False   False
0x0a577020 smss.exe                364 True   True   True     True   False False   False
0x0a56d6e8 csrss.exe               588 True   True   True     True   False True    True
0x0a65ba20 Newfile.exe            3892 False  True   False    False  False False   False    2020-01-25 08:11:09 UTC+0
000
0x0a65e1a8 cmd.exe                3884 False  True   False    False  False False   False    2020-01-25 08:11:09 UTC+0
000

C:\Users\IEUser\Desktop
λ volatility.exe -f TESTED-08375-20200125-081134.raw --profile=WinXPSP3x86 apihooks
Volatility Foundation Volatility Framework 2.6
Interrupted

C:\Users\IEUser\Desktop
λ volatility.exe -f TESTED-08375-20200125-081134.raw --profile=WinXPSP3x86 apihooks -p 3892
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : Cannot find PID 3892. If its terminated or unlinked, use psscan and then supply --off
set=OFFSET

C:\Users\IEUser\Desktop
λ volatility.exe -f TESTED-08375-20200125-081134.raw --profile=WinXPSP3x86 apihooks --offset=0x0a65ba20
Volatility Foundation Volatility Framework 2.6

C:\Users\IEUser\Desktop
λ volatility.exe -f TESTED-08375-20200125-081134.raw --profile=WinXPSP3x86 apihooks --offset=0x0a65e1a8
Volatility Foundation Volatility Framework 2.6

C:\Users\IEUser\Desktop
λ |
```

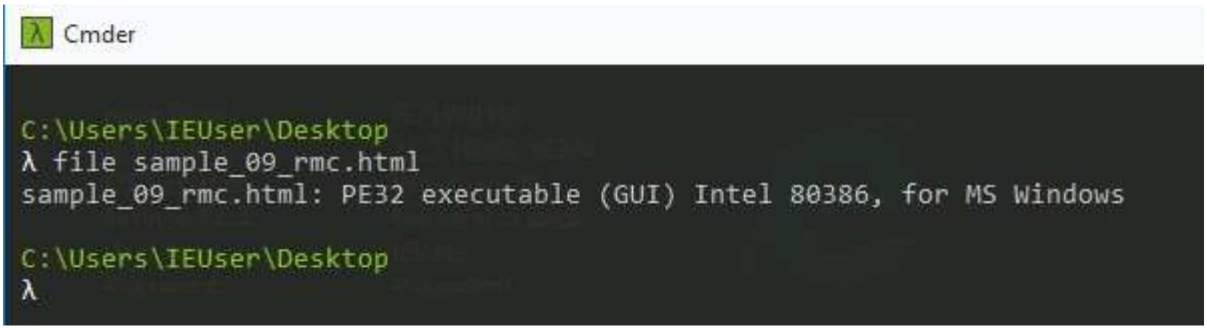
13. Does this malware propagate/spread itself?

14. 14- Write a script/program to clean an infected system automatically. If you aren't able to do it, show the manual steps

1- main page
2- table of content
3- synthesis
4- identification => sha256, file, strings, CFF Explorer
5- dynamic analysis => procmon, procexp, network trafic, memory dump generation
6- memory forensics analysis
7- disinfection

The memory analysis part should answer the following questions (if applicable):

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



```
C:\Users\IEUser\Desktop
λ file sample_09_rmc.html
sample_09_rmc.html: PE32 executable (GUI) Intel 80386, for MS Windows

C:\Users\IEUser\Desktop
λ
```

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

3- Which process is making network connections?
4- Where are the remote IP addresses/domain name located?
5- Find where the malicious program is recorded in the registry startup list
6- What's the SHA256 of this malware?
7- What are the sections of this PE file?
8- Any interesting strings from this malware?

9- How does this malware executes its code on the system? dump it.
10- What is this malware's name?
11- Give its mutexes.
12- What are the hooked API? From which processes?
13- Does this malware propagate/spread itself?
14- Write a script/program to clean an infected system automatically. If you aren't able to do it, show the manual steps