Malware Analysis

Executive Summary

The file is a sample of the ransomware called Crysis. It functions by encrypting all the files present in the user's system drives and prompts him to provide monetary compensation if he requires decryption. The amount of money demanded as ransom supposedly increases proportionate to the amount of time the user takes to respond to the malicious attackers. The sample is heavily encrypted in itself, trying to obfuscate any attempts at analysis. Most of the functionality is observed dynamically on execution of the ransomware. The information presented below is a concise representation of the analysis done on the malware.

Basic Static Analysis

The program is not packed as inferred from PeiD. In addition, we can observe that the virtual size and the raw data size of the .text section are roughly the same further confirming that the program is unpacked. The malware was compiled on the 26th of february 2017 at 6:27 AM UTC as seen from PEview and is a Windows GUI application. This particular sample has an MD5 hash of 20D021DDCDCC32CB79F528DBB45E2207.

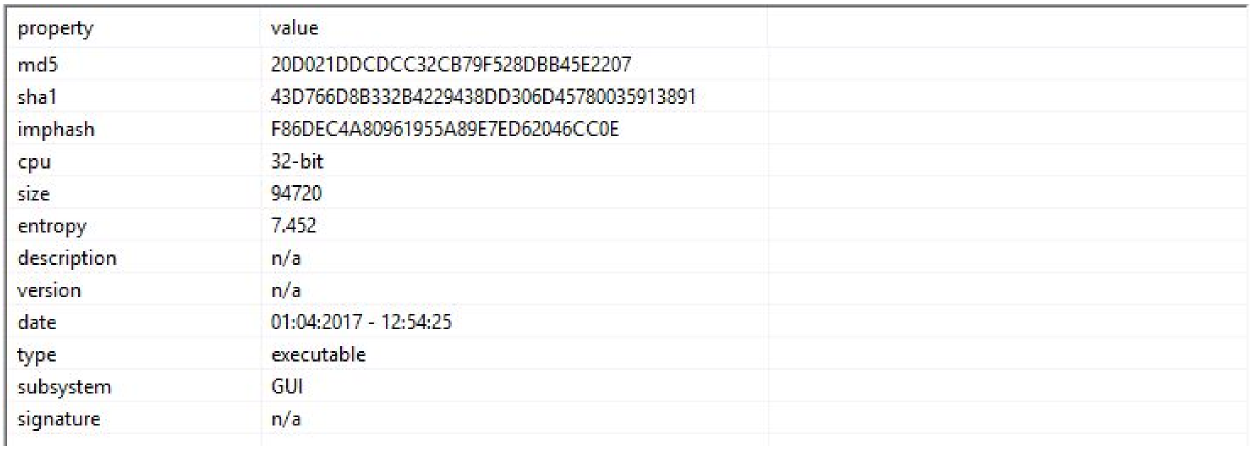
The malware sample seems to be heavily encrypted as most of the information that can be inferred via static analysis seems to be heavily obfuscated.

The sample shows no resources on examining it with Resource Hacker. The sample only has 3 visible sections whose contents are presented below.

The sample also displays very few imports and strings for a malware sample when viewed using PEStudio. Though this suggests that the malware may be packed, we mentioned previously that it does not appear to be so. On further investigating the available imports, we see 2 notable imports “GetProcAddress” and “LoadLibraryA”. This suggests that the malware may possibly be dynamically importing the functions required for its working and building its own IAT during its execution. We investigate this further in the dynamic analysis section.

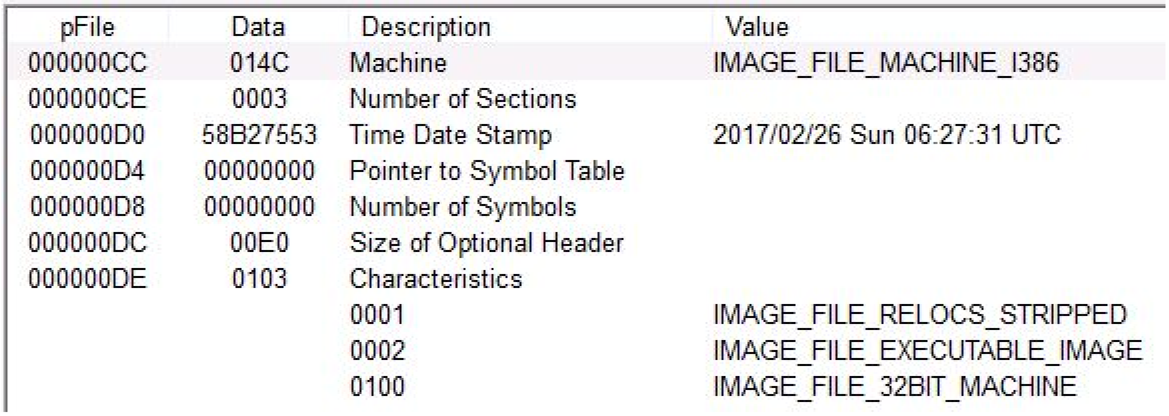
The only notable string is the ASCII value “C:\crysis\Release\PDB\payload.pdb”. This provides some credence to the claim that the ransomware belongs to the Crysis family of Malware.

We look further into these findings in the upcoming sections.



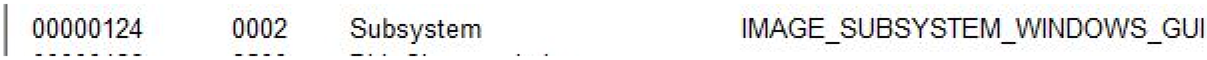
property	value
md5	20D021DDCDCC32CB79F528DBB45E2207
sha1	43D766D8B332B4229438DD306D45780035913891
imphash	F86DEC4A80961955A89E7ED62046CC0E
cpu	32-bit
size	94720
entropy	7.452
description	n/a
version	n/a
date	01:04:2017 - 12:54:25
type	executable
subsystem	GUI
signature	n/a

Fig.1 General Info



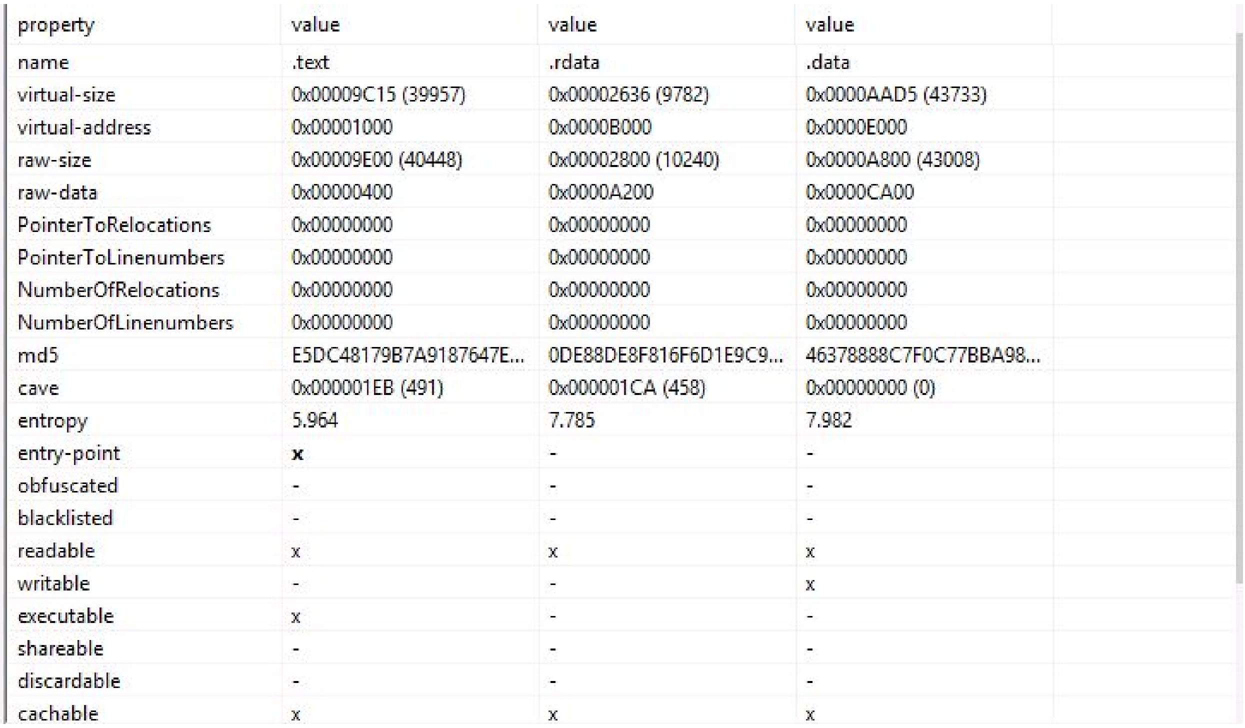
pFile	Data	Description	Value
000000CC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000CE	0003	Number of Sections	
000000D0	58B27553	Time Date Stamp	2017/02/26 Sun 06:27:31 UTC
000000D4	00000000	Pointer to Symbol Table	
000000D8	00000000	Number of Symbols	
000000DC	00E0	Size of Optional Header	
000000DE	0103	Characteristics	
		0001	IMAGE_FILE_RELOCS_STRIPPED
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0100	IMAGE_FILE_32BIT_MACHINE

Fig.2 Compile date



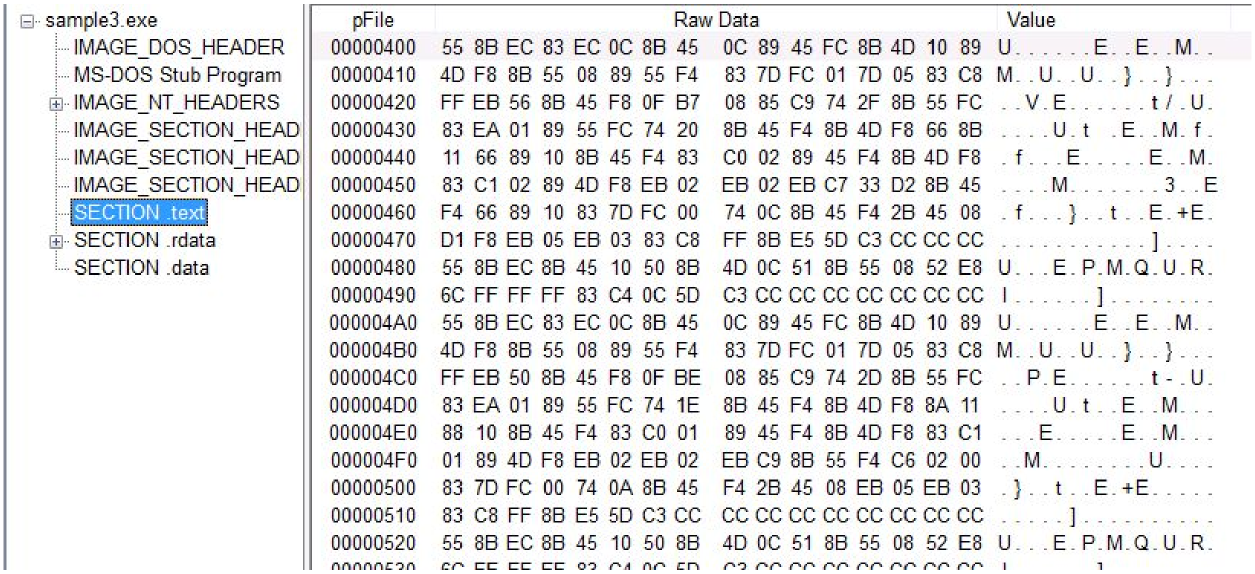
00000124	0002	Subsystem	IMAGE_SUBSYSTEM_WINDOWS_GUI

Fig.3 Windows GUI



property	value	value	value	
name	.text	.rdata	.data	
virtual-size	0x00009C15 (39957)	0x00002636 (9782)	0x0000AAD5 (43733)	
virtual-address	0x00001000	0x0000B000	0x0000E000	
raw-size	0x00009E00 (40448)	0x00002800 (10240)	0x0000A800 (43008)	
raw-data	0x00000400	0x0000A200	0x0000CA00	
PointerToRelocations	0x00000000	0x00000000	0x00000000	
PointerToLinenumbers	0x00000000	0x00000000	0x00000000	
NumberOfRelocations	0x00000000	0x00000000	0x00000000	
NumberOfLinenumbers	0x00000000	0x00000000	0x00000000	
md5	E5DC48179B7A9187647E...	0DE88DE8F816F6D1E9C9...	46378888C7F0C77BBA98...	
cave	0x000001EB (491)	0x000001CA (458)	0x00000000 (0)	
entropy	5.964	7.785	7.982	
entry-point	**x**	-	-	
obfuscated	-	-	-	
blacklisted	-	-	-	
readable	x	x	x	
writable	-	-	x	
executable	x	-	-	
shareable	-	-	-	
discardable	-	-	-	
cachable	x	x	x	

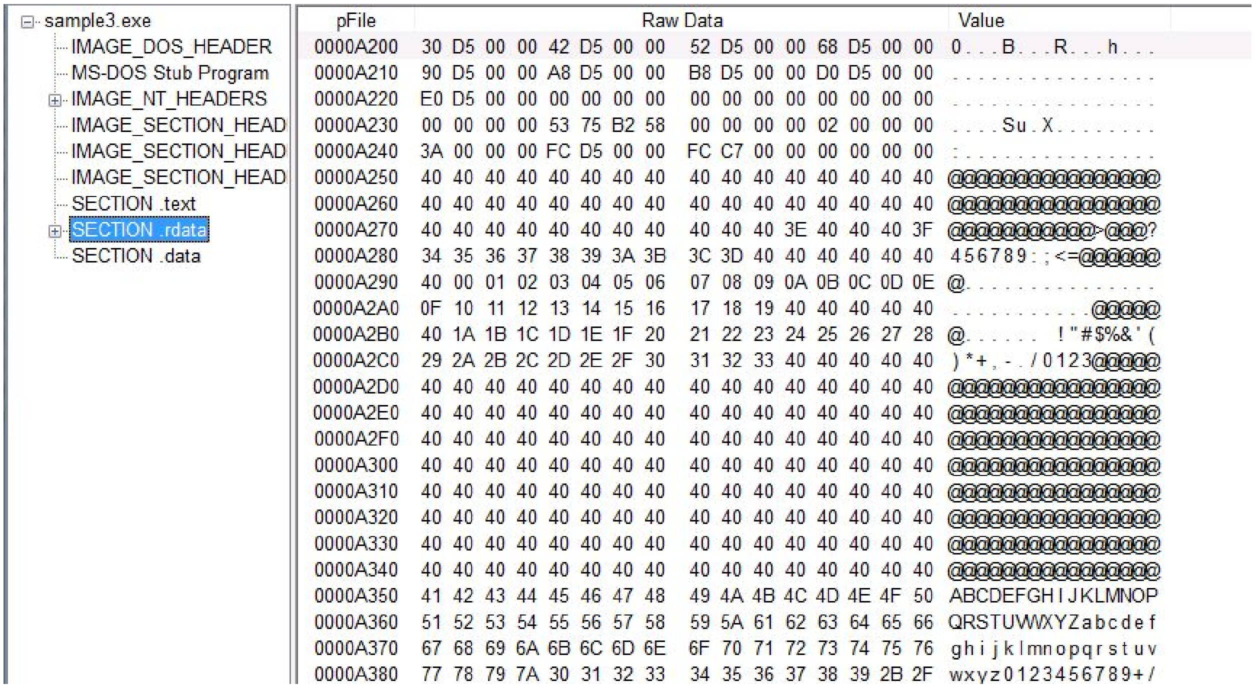
Fig. 4 Sections



```
sample3.exe
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
  IMAGE_SECTION_HEAD
  IMAGE_SECTION_HEAD
  IMAGE_SECTION_HEAD
  SECTION .text
  SECTION .rdata
  SECTION .data
```

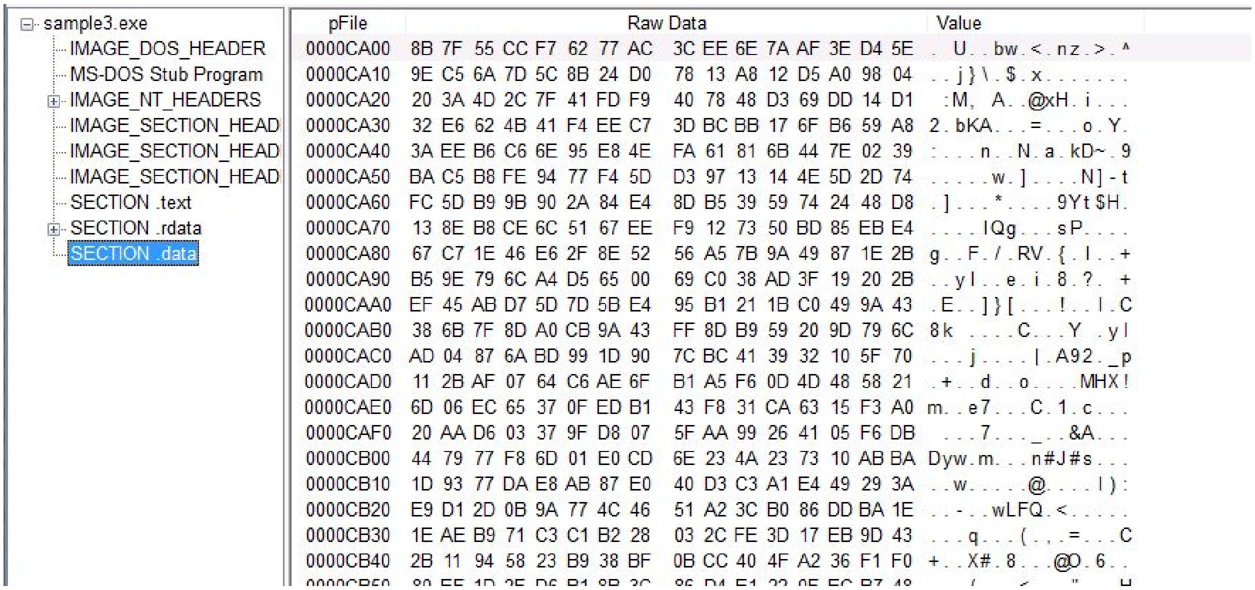
```
pFile     Raw Data                                         Value
00000400  55 8B EC 83 EC 0C 8B 45  0C 89 45 FC 8B 4D 10 89  U.......E..E..M..
00000410  4D F8 8B 55 08 89 55 F4  83 7D FC 01 7D 05 83 C8  M..U..U..}..}...
00000420  FF EB 56 8B 45 F8 0F B7  08 85 C9 74 2F 8B 55 FC  ..V.E......t/.U.
00000430  83 EA 01 89 55 FC 74 20  8B 45 F4 8B 4D F8 66 8B  ....U.t .E..M.f.
00000440  11 66 89 10 8B 45 F4 83  C0 02 89 45 F4 8B 4D F8  .f...E.....E..M.
00000450  83 C1 02 89 4D F8 EB 02  EB 02 EB C7 33 D2 8B 45  ....M.......3..E
00000460  F4 66 89 10 83 7D FC 00  74 0C 8B 45 F4 2B 45 08  .f...}..t..E.+E.
00000470  D1 F8 EB 05 EB 03 83 C8  FF 8B E5 5D C3 CC CC CC  ............]....
00000480  55 8B EC 8B 45 10 50 8B  4D 0C 51 8B 55 08 52 E8  U...E.P.M.Q.U.R.
00000490  6C FF FF FF 83 C4 0C 5D  C3 CC CC CC CC CC CC CC  l.......].......
000004A0  55 8B EC 83 EC 0C 8B 45  0C 89 45 FC 8B 4D 10 89  U.......E..E..M..
000004B0  4D F8 8B 55 08 89 55 F4  83 7D FC 01 7D 05 83 C8  M..U..U..}..}...
000004C0  FF EB 50 8B 45 F8 0F BE  08 85 C9 74 2D 8B 55 FC  ..P.E......t-.U.
000004D0  83 EA 01 89 55 FC 74 1E  8B 45 F4 8B 4D F8 8A 11  ....U.t..E..M...
000004E0  88 10 8B 45 F4 83 C0 01  89 45 F4 8B 4D F8 83 C1  ...E.....E..M...
000004F0  01 89 4D F8 EB 02 EB 02  EB C9 8B 55 F4 C6 02 00  ..M.........U....
00000500  83 7D FC 00 74 0A 8B 45  F4 2B 45 08 EB 05 EB 03  .}..t..E.+E.....
00000510  83 C8 FF 8B E5 5D C3 CC  CC CC CC CC CC CC CC CC  ......]..........
00000520  55 8B EC 8B 45 10 50 8B  4D 0C 51 8B 55 08 52 E8  U...E.P.M.Q.U.R.
```

Fig.5 .text section



```
pFile     Raw Data                                          Value
0000A200  30 D5 00 00 42 D5 00 00  52 D5 00 00 68 D5 00 00  0...B...R...h...
0000A210  90 D5 00 00 A8 D5 00 00  B8 D5 00 00 D0 D5 00 00  ................
0000A220  E0 D5 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0000A230  00 00 00 00 53 75 B2 58  00 00 00 00 02 00 00 00  ....Su.X........
0000A240  3A 00 00 00 FC D5 00 00  FC C7 00 00 00 00 00 00  :...............
0000A250  40 40 40 40 40 40 40 40  40 40 40 40 40 40 40 40  @@@@@@@@@@@@@@@@
0000A260  40 40 40 40 40 40 40 40  40 40 40 40 40 40 40 40  @@@@@@@@@@@@@@@@
0000A270  40 40 40 40 40 40 40 40  40 40 40 3E 40 40 40 3F  @@@@@@@@@@@>@@@?
0000A280  34 35 36 37 38 39 3A 3B  3C 3D 40 40 40 40 40 40  456789:;<=@@@@@@
0000A290  40 00 01 02 03 04 05 06  07 08 09 0A 0B 0C 0D 0E  @...............
0000A2A0  0F 10 11 12 13 14 15 16  17 18 19 40 40 40 40 40  ...........@@@@@
0000A2B0  40 1A 1B 1C 1D 1E 1F 20  21 22 23 24 25 26 27 28  @...... !"#$%&'(
0000A2C0  29 2A 2B 2C 2D 2E 2F 30  31 32 33 40 40 40 40 40  )*+,-./0123@@@@@
0000A2D0  40 40 40 40 40 40 40 40  40 40 40 40 40 40 40 40  @@@@@@@@@@@@@@@@
0000A2E0  40 40 40 40 40 40 40 40  40 40 40 40 40 40 40 40  @@@@@@@@@@@@@@@@
0000A2F0  40 40 40 40 40 40 40 40  40 40 40 40 40 40 40 40  @@@@@@@@@@@@@@@@
0000A300  40 40 40 40 40 40 40 40  40 40 40 40 40 40 40 40  @@@@@@@@@@@@@@@@
0000A310  40 40 40 40 40 40 40 40  40 40 40 40 40 40 40 40  @@@@@@@@@@@@@@@@
0000A320  40 40 40 40 40 40 40 40  40 40 40 40 40 40 40 40  @@@@@@@@@@@@@@@@
0000A330  40 40 40 40 40 40 40 40  40 40 40 40 40 40 40 40  @@@@@@@@@@@@@@@@
0000A340  40 40 40 40 40 40 40 40  40 40 40 40 40 40 40 40  @@@@@@@@@@@@@@@@
0000A350  41 42 43 44 45 46 47 48  49 4A 4B 4C 4D 4E 4F 50  ABCDEFGHIJKLMNOP
0000A360  51 52 53 54 55 56 57 58  59 5A 61 62 63 64 65 66  QRSTUVWXYZabcdef
0000A370  67 68 69 6A 6B 6C 6D 6E  6F 70 71 72 73 74 75 76  ghijklmnopqrstuv
0000A380  77 78 79 7A 30 31 32 33  34 35 36 37 38 39 2B 2F  wxyz0123456789+/
```

Fig.6 .rdata section



```
pFile     Raw Data                                          Value
0000CA00  8B 7F 55 CC F7 62 77 AC  3C EE 6E 7A AF 3E D4 5E  ..U..bw.<.nz.>.^
0000CA10  9E C5 6A 7D 5C 8B 24 D0  78 13 A8 12 D5 A0 98 04  ..j}\.$.x.......
0000CA20  20 3A 4D 2C 7F 41 FD F9  40 78 48 D3 69 DD 14 D1   :M,.A..@xH.i...
0000CA30  32 E6 62 4B 41 F4 EE C7  3D BC BB 17 6F B6 59 A8  2.bKA...=...o.Y.
0000CA40  3A EE B6 C6 6E 95 E8 4E  FA 61 81 6B 44 7E 02 39  :...n..N.a.kD~.9
0000CA50  BA C5 B8 FE 94 77 F4 5D  D3 97 13 14 4E 5D 2D 74  .....w.]....N]-t
0000CA60  FC 5D B9 9B 90 2A 84 E4  8D B5 39 59 74 24 48 D8  .]...*....9Yt$H.
0000CA70  13 8E B8 CE 6C 51 67 EE  F9 12 73 50 BD 85 EB E4  ....lQg...sP....
0000CA80  67 C7 1E 46 E6 2F 8E 52  56 A5 7B 9A 49 87 1E 2B  g..F./.RV.{.I..+
0000CA90  B5 9E 79 6C A4 D5 65 00  69 C0 38 AD 3F 19 20 2B  ..yl..e.i.8.?. +
0000CAA0  EF 45 AB D7 5D 7D 5B E4  95 B1 21 1B C0 49 9A 43  .E..]}[...!..I.C
0000CAB0  38 6B 7F 8D A0 CB 9A 43  FF 8D B9 59 20 9D 79 6C  8k.....C...Y .yl
0000CAC0  AD 04 87 6A BD 99 1D 90  7C BC 41 39 32 10 5F 70  ...j....|.A92._p
0000CAD0  11 2B AF 07 64 C6 AE 6F  B1 A5 F6 0D 4D 48 58 21  .+..d..o....MHX!
0000CAE0  6D 06 EC 65 37 0F ED B1  43 F8 31 CA 63 15 F3 A0  m..e7...C.1.c...
0000CAF0  20 AA D6 03 37 9F D8 07  5F AA 99 26 41 05 F6 DB   ...7..._..&A...
0000CB00  44 79 77 F8 6D 01 E0 CD  6E 23 4A 23 73 10 AB BA  Dyw.m...n#J#s...
0000CB10  1D 93 77 DA E8 AB 87 E0  40 D3 C3 A1 E4 49 29 3A  ..w.....@....I):
0000CB20  E9 D1 2D 0B 9A 77 4C 46  51 A2 3C B0 86 DD BA 1E  ..-..wLFQ.<.....
0000CB30  1E AE B9 71 C3 C1 B2 28  03 2C FE 3D 17 EB 9D 43  ...q...(.,.=...C
0000CB40  2B 11 94 58 23 B9 38 BF  0B CC 40 4F A2 36 F1 F0  +..X#.8...@O.6..
```

Fig.7 .data section

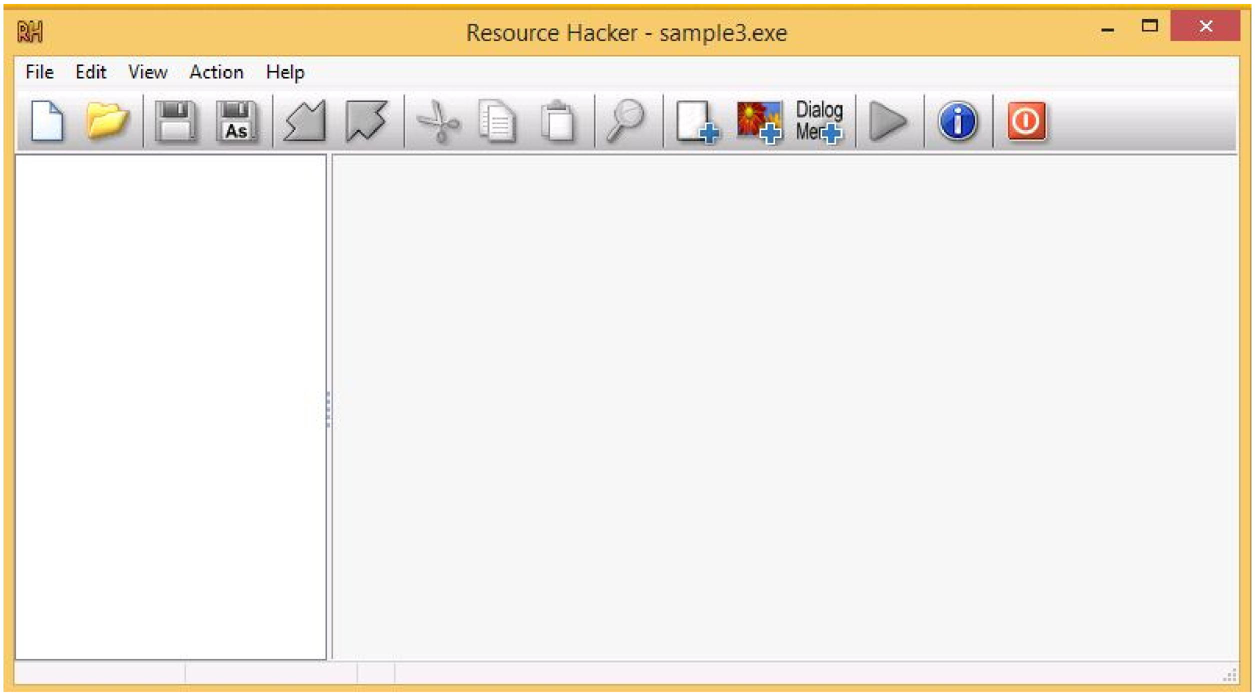
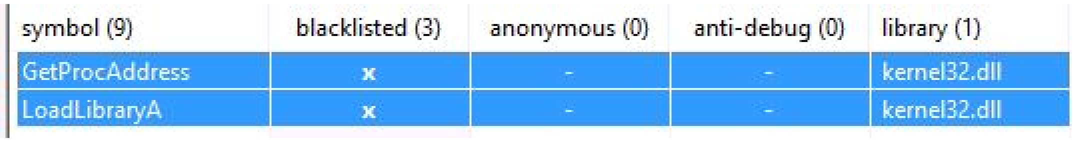
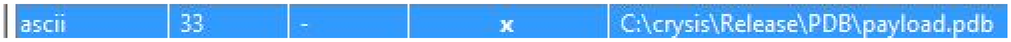


Fig.8 Resource hacker



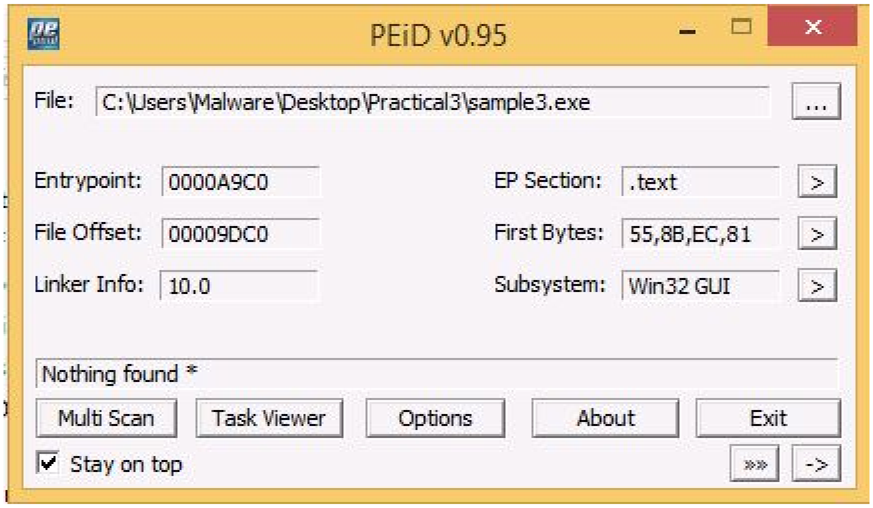
symbol (9)	blacklisted (3)	anonymous (0)	anti-debug (0)	library (1)
GetProcAddress	x	-	-	kernel32.dll
LoadLibraryA	x	-	-	kernel32.dll

Fig.10 Imports



ascii	33	-	x	C:\crysis\Release\PDB\payload.pdb

Fig.9 Strings



PEiD v0.95

File: C:\Users\Malware\Desktop\Practical3\sample3.exe

Entrypoint: 0000A9C0

EP Section: .text

File Offset: 00009DC0

First Bytes: 55,8B,EC,81

Linker Info: 10.0

Subsystem: Win32 GUI

Nothing found *

☑ Stay on top

Fig.10 PEiD

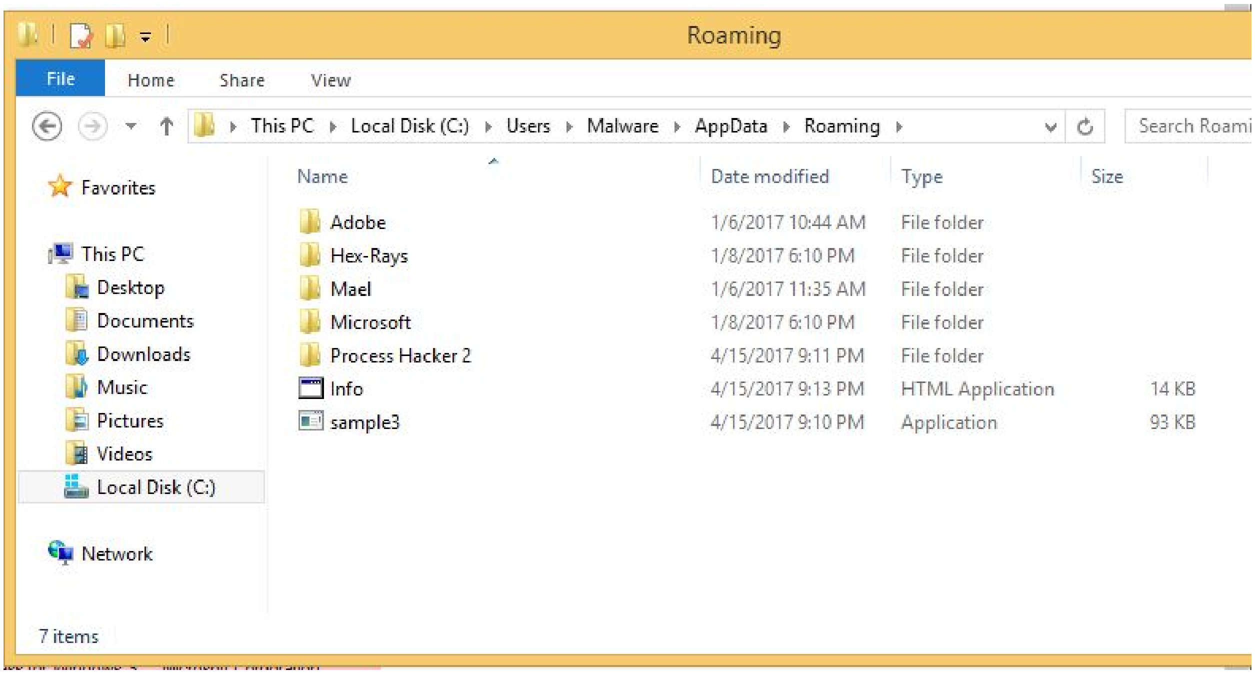
Basic Dynamic Analysis

Sample3.exe when it is first run, hides its presence from the user by creating a secondary executable and then deleting the initial executable file from the system. The secondary executable is hidden in the system and the typical user is not aware of its existence until it becomes active. The malware creates the secondary file in \AppData as shown below. It also appends itself in the system start menu. The Malware on execution, launches 2 processes, vssadmin.exe and conhost.exe under cmd.exe. This implies that the malware runs some shell commands using the command prompt. While conhost.exe is a legitimate process that fixes some windows bugs existing in prior versions, it could also be subject to code injection by the sample malware.

The more dangerous process is vssadmin.exe. Vssadmin.exe is a process in windows that allows an administrator to manage the Shadow Volume Copies that are on the computer. The shadow volume copies are backups or snapshots that allow you to restore your system to an earlier point. The malware attempts to delete the Shadow Volume Copies using Vssadmin.exe therefore preventing any capability to restore the system to an earlier point. The program also launches vssvc.exe which is another process that manipulates the shadow volume copies. Once these processes are launched, the malware then chooses files on random in the file system directory and creates a new encrypted version of them, saving the encrypted copy with a new file extension and deleting the original file as can be seen using procmon. The file extension is the same for every file and follows “filename.id-68672ACE.[mk.raiden@aol.com]” as can be seen below.

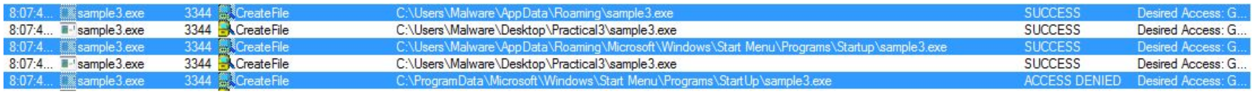
We see using Procmon that the malware loads a large number of dlls upon execution further solidifying the fact that it attempts to construct its own IAT dynamically. Though the malware imports several network dlls like “netutils.dll”, “urlmon.dll” and “ws2_32.dll”, it does not seem to depend on network communication to do the encryption. In other words, the malware does in place encryption and does not require any key exchange with a command and control server. Infact no communication is observed and if any is present, it can be assumed that the malware

simply communicates its status along with the infected system information. We also see a number of crypto libraries being imported like “cryptbase.dll”, “bcryptprimitives.dll”, “cryptsp.dll” and “rsaenh.dll” whose functionality is being used in the encryption process. The entire list of libraries imported is presented below.
The malware also portrays a lot of registry activity as is expected. In particular, it adds a registry value “HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\sample3.exe: “C:\Windows\System32\sample3.exe” “. This value ensures persistence of the malware across reboots. We also see a number of keys or values corresponding to the VSS updated. There are a few keys implying deletion of snapshots. The entire registry change are shown below.
Upon completely encrypting the entire system, the malware then launches a process “mshta.exe” which spawns a page that tells the user that his system has been encrypted. It gives him instructions on how to purchase bitcoin and where to send it to. It also informs him about some details pertaining to the decryption followed by several warnings. A text file is also created on the desktop with the title “INFORMATION HOW TO recovery PC” which explains with broken english that the user’s files have been encrypted.
On viewing the file system directories, we see that all files have been encrypted with a “.wallet” extension. The structure of each of these files and more is investigated in the advanced analysis section.



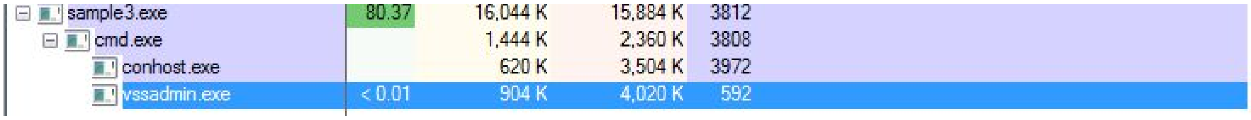
Name	Date modified	Type	Size
Adobe	1/6/2017 10:44 AM	File folder	
Hex-Rays	1/8/2017 6:10 PM	File folder	
Mael	1/6/2017 11:35 AM	File folder	
Microsoft	1/8/2017 6:10 PM	File folder	
Process Hacker 2	4/15/2017 9:11 PM	File folder	
Info	4/15/2017 9:13 PM	HTML Application	14 KB
sample3	4/15/2017 9:10 PM	Application	93 KB

Fig.11 New sample created



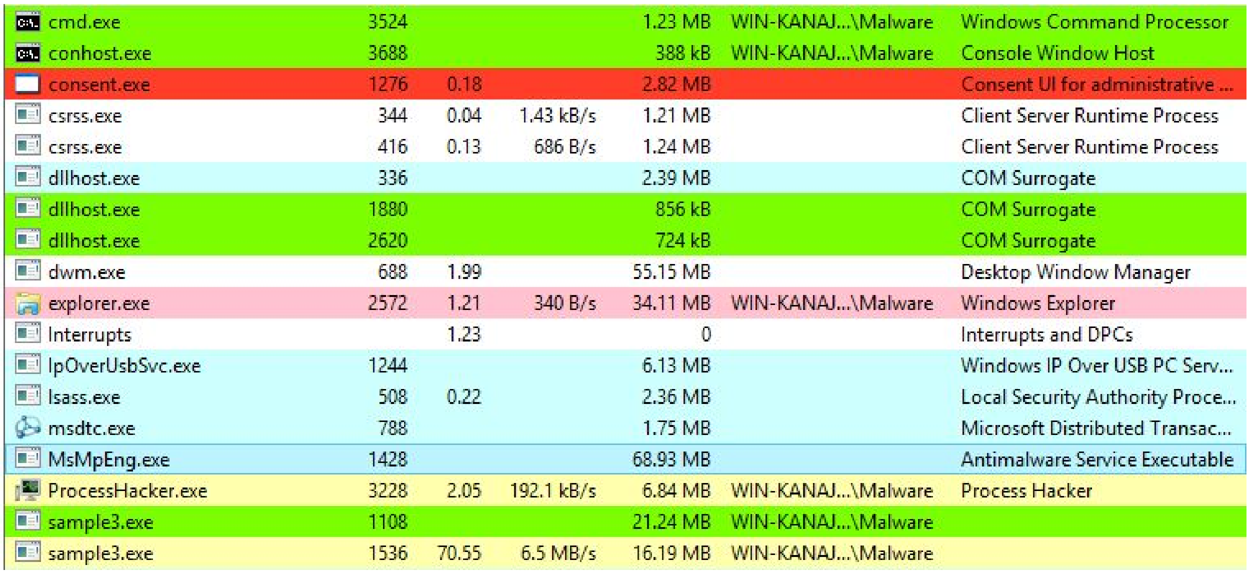
8:07:4...	sample3.exe	3344	CreateFile	C:\Users\Malware\AppData\Roaming\sample3.exe	SUCCESS	Desired Access: G...
8:07:4...	sample3.exe	3344	CreateFile	C:\Users\Malware\Desktop\Practical3\sample3.exe	SUCCESS	Desired Access: G...
8:07:4...	sample3.exe	3344	CreateFile	C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\sample3.exe	SUCCESS	Desired Access: G...
8:07:4...	sample3.exe	3344	CreateFile	C:\Users\Malware\Desktop\Practical3\sample3.exe	SUCCESS	Desired Access: G...
8:07:4...	sample3.exe	3344	CreateFile	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\sample3.exe	ACCESS DENIED	Desired Access: G...

Fig.12 Appending to the start menu



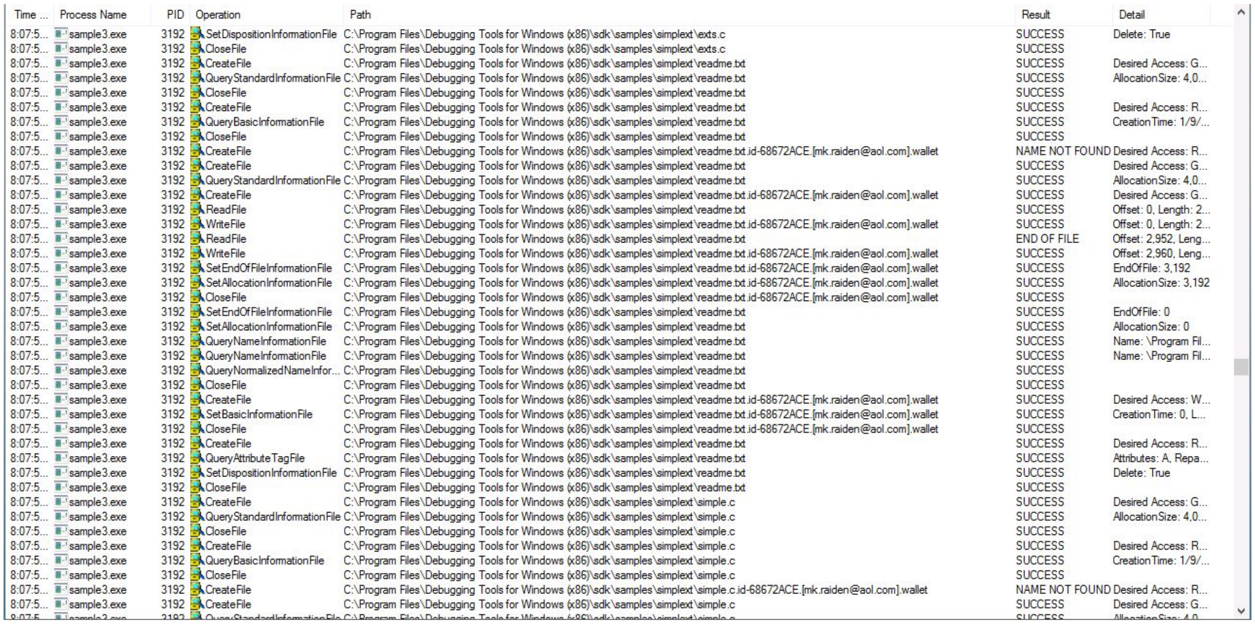
sample3.exe	80.37	16,044 K	15,884 K	3812
cmd.exe		1,444 K	2,360 K	3808
conhost.exe		620 K	3,504 K	3972
vssadmin.exe	< 0.01	904 K	4,020 K	592

Fig.13.1 New processes spawned



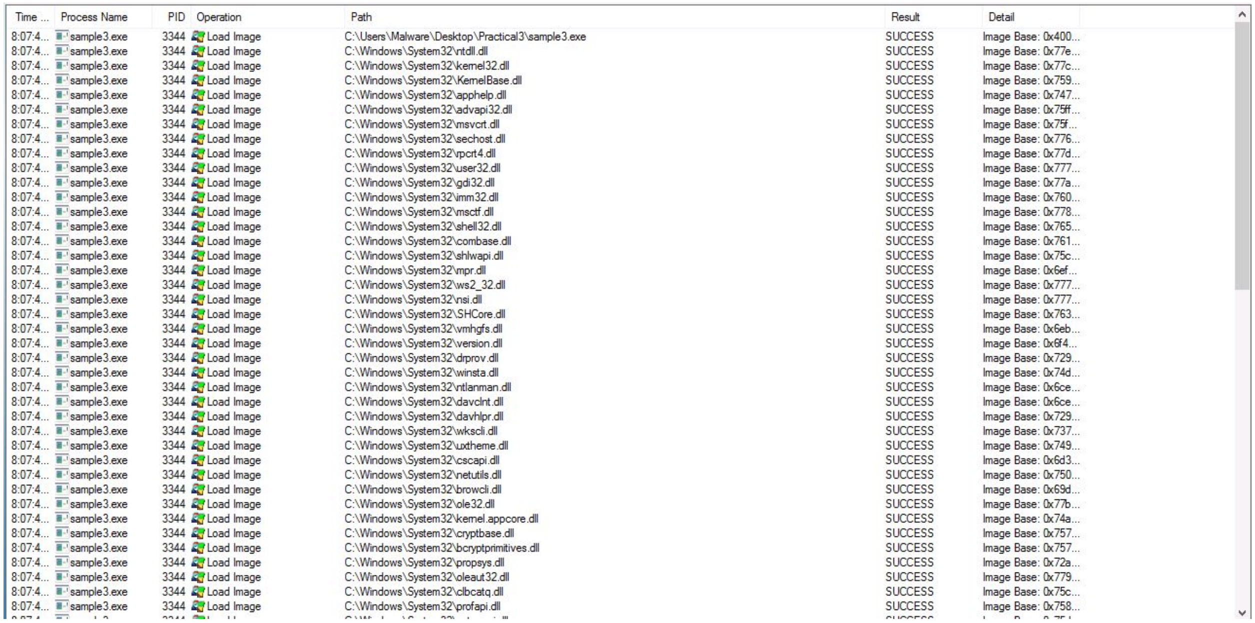
cmd.exe	3524			1.23 MB	WIN-KANAJ...\Malware	Windows Command Processor
conhost.exe	3688			388 kB	WIN-KANAJ...\Malware	Console Window Host
consent.exe	1276	0.18		2.82 MB		Consent UI for administrative ...
csrss.exe	344	0.04	1.43 kB/s	1.21 MB		Client Server Runtime Process
csrss.exe	416	0.13	686 B/s	1.24 MB		Client Server Runtime Process
dllhost.exe	336			2.39 MB		COM Surrogate
dllhost.exe	1880			856 kB		COM Surrogate
dllhost.exe	2620			724 kB		COM Surrogate
dwm.exe	688	1.99		55.15 MB		Desktop Window Manager
explorer.exe	2572	1.21	340 B/s	34.11 MB	WIN-KANAJ...\Malware	Windows Explorer
Interrupts		1.23		0		Interrupts and DPCs
IpOverUsbSvc.exe	1244			6.13 MB		Windows IP Over USB PC Serv...
lsass.exe	508	0.22		2.36 MB		Local Security Authority Proce...
msdtc.exe	788			1.75 MB		Microsoft Distributed Transac...
MsMpEng.exe	1428			68.93 MB		Antimalware Service Executable
ProcessHacker.exe	3228	2.05	192.1 kB/s	6.84 MB	WIN-KANAJ...\Malware	Process Hacker
sample3.exe	1108			21.24 MB	WIN-KANAJ...\Malware	
sample3.exe	1536	70.55	6.5 MB/s	16.19 MB	WIN-KANAJ...\Malware	

Fig.13.2 New processes spawned



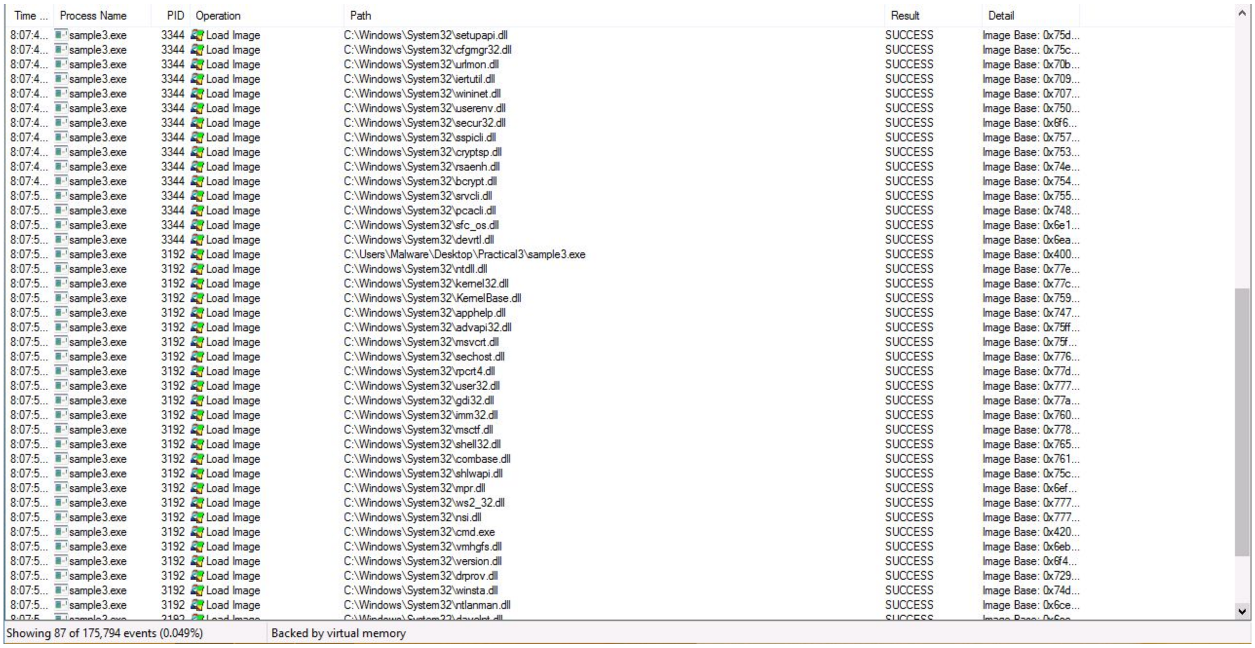
Time ...	Process Name	PID	Operation	Path	Result	Detail
8:07:5...	sample3.exe	3192	SetDispositionInformationFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\exts.c	SUCCESS	Delete: True
8:07:5...	sample3.exe	3192	CloseFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\exts.c	SUCCESS	
8:07:5...	sample3.exe	3192	CreateFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	Desired Access: G...
8:07:5...	sample3.exe	3192	QueryStandardInformationFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	AllocationSize: 4,0...
8:07:5...	sample3.exe	3192	CloseFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	
8:07:5...	sample3.exe	3192	CreateFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	Desired Access: R...
8:07:5...	sample3.exe	3192	QueryBasicInformationFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	CreationTime: 1/9/...
8:07:5...	sample3.exe	3192	CloseFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	
8:07:5...	sample3.exe	3192	CreateFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt.id-68672ACE.[mk.raiden@aol.com].wallet	NAME NOT FOUND	Desired Access: R...
8:07:5...	sample3.exe	3192	CreateFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	Desired Access: G...
8:07:5...	sample3.exe	3192	QueryStandardInformationFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	AllocationSize: 4,0...
8:07:5...	sample3.exe	3192	CreateFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt.id-68672ACE.[mk.raiden@aol.com].wallet	SUCCESS	Desired Access: G...
8:07:5...	sample3.exe	3192	ReadFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	Offset: 0, Length: 2...
8:07:5...	sample3.exe	3192	WriteFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt.id-68672ACE.[mk.raiden@aol.com].wallet	SUCCESS	Offset: 0, Length: 2...
8:07:5...	sample3.exe	3192	ReadFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	END OF FILE	Offset: 2,952, Leng...
8:07:5...	sample3.exe	3192	WriteFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt.id-68672ACE.[mk.raiden@aol.com].wallet	SUCCESS	Offset: 2,960, Leng...
8:07:5...	sample3.exe	3192	SetEndOfFileInformationFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt.id-68672ACE.[mk.raiden@aol.com].wallet	SUCCESS	EndOfFile: 3,192
8:07:5...	sample3.exe	3192	SetAllocationInformationFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt.id-68672ACE.[mk.raiden@aol.com].wallet	SUCCESS	AllocationSize: 3,192
8:07:5...	sample3.exe	3192	CloseFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt.id-68672ACE.[mk.raiden@aol.com].wallet	SUCCESS	
8:07:5...	sample3.exe	3192	SetEndOfFileInformationFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	EndOfFile: 0
8:07:5...	sample3.exe	3192	SetAllocationInformationFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	AllocationSize: 0
8:07:5...	sample3.exe	3192	QueryNameInformationFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	Name: \Program Fil...
8:07:5...	sample3.exe	3192	QueryNameInformationFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	Name: \Program Fil...
8:07:5...	sample3.exe	3192	QueryNormalizedNameInfor...	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	
8:07:5...	sample3.exe	3192	CloseFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	
8:07:5...	sample3.exe	3192	CreateFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt.id-68672ACE.[mk.raiden@aol.com].wallet	SUCCESS	Desired Access: W...
8:07:5...	sample3.exe	3192	SetBasicInformationFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt.id-68672ACE.[mk.raiden@aol.com].wallet	SUCCESS	CreationTime: 0, L...
8:07:5...	sample3.exe	3192	CloseFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt.id-68672ACE.[mk.raiden@aol.com].wallet	SUCCESS	
8:07:5...	sample3.exe	3192	CreateFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	Desired Access: R...
8:07:5...	sample3.exe	3192	QueryAttributeTagFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	Attributes: A, Repa...
8:07:5...	sample3.exe	3192	SetDispositionInformationFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	Delete: True
8:07:5...	sample3.exe	3192	CloseFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\readme.txt	SUCCESS	
8:07:5...	sample3.exe	3192	CreateFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\simple.c	SUCCESS	Desired Access: G...
8:07:5...	sample3.exe	3192	QueryStandardInformationFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\simple.c	SUCCESS	AllocationSize: 4,0...
8:07:5...	sample3.exe	3192	CloseFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\simple.c	SUCCESS	
8:07:5...	sample3.exe	3192	CreateFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\simple.c	SUCCESS	Desired Access: R...
8:07:5...	sample3.exe	3192	QueryBasicInformationFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\simple.c	SUCCESS	CreationTime: 1/9/...
8:07:5...	sample3.exe	3192	CloseFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\simple.c	SUCCESS	
8:07:5...	sample3.exe	3192	CreateFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\simple.c.id-68672ACE.[mk.raiden@aol.com].wallet	NAME NOT FOUND	Desired Access: R...
8:07:5...	sample3.exe	3192	CreateFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\simple.c	SUCCESS	Desired Access: G...
8:07:5...	sample3.exe	3192	QueryStandardInformationFile	C:\Program Files\Debugging Tools for Windows (x86)\sdk\samples\simplext\simple.c	SUCCESS	AllocationSize: 4,0...

Fig.14 Creation of encrypted files



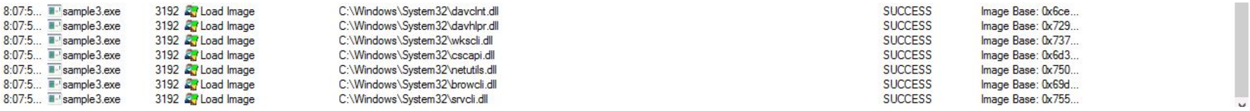
```
Time ...  Process Name   PID   Operation    Path                                              Result    Detail
8:07:4... sample3.exe    3344  Load Image   C:\Users\Malware\Desktop\Practical3\sample3.exe   SUCCESS   Image Base: 0x400...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\ntdll.dll                     SUCCESS   Image Base: 0x77e...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\kernel32.dll                  SUCCESS   Image Base: 0x77c...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\KernelBase.dll                SUCCESS   Image Base: 0x759...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\apphelp.dll                   SUCCESS   Image Base: 0x747...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\advapi32.dll                  SUCCESS   Image Base: 0x75ff...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\msvcrt.dll                    SUCCESS   Image Base: 0x75f...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\sechost.dll                   SUCCESS   Image Base: 0x776...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\rpcrt4.dll                    SUCCESS   Image Base: 0x77d...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\user32.dll                    SUCCESS   Image Base: 0x777...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\gdi32.dll                     SUCCESS   Image Base: 0x77a...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\imm32.dll                     SUCCESS   Image Base: 0x760...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\msctf.dll                     SUCCESS   Image Base: 0x778...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\shell32.dll                   SUCCESS   Image Base: 0x765...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\combase.dll                   SUCCESS   Image Base: 0x761...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\shlwapi.dll                   SUCCESS   Image Base: 0x75c...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\mpr.dll                       SUCCESS   Image Base: 0x6ef...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\ws2_32.dll                    SUCCESS   Image Base: 0x777...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\nsi.dll                       SUCCESS   Image Base: 0x777...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\SHCore.dll                    SUCCESS   Image Base: 0x763...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\vmhgfs.dll                    SUCCESS   Image Base: 0x6eb...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\version.dll                   SUCCESS   Image Base: 0x6f4...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\drprov.dll                    SUCCESS   Image Base: 0x729...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\winsta.dll                    SUCCESS   Image Base: 0x74d...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\ntlanman.dll                  SUCCESS   Image Base: 0x6ce...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\davclnt.dll                   SUCCESS   Image Base: 0x6ce...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\davhlpr.dll                   SUCCESS   Image Base: 0x729...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\wkscli.dll                    SUCCESS   Image Base: 0x737...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\uxtheme.dll                   SUCCESS   Image Base: 0x749...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\cscapi.dll                    SUCCESS   Image Base: 0x6d3...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\netutils.dll                  SUCCESS   Image Base: 0x750...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\browcli.dll                   SUCCESS   Image Base: 0x69d...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\ole32.dll                     SUCCESS   Image Base: 0x77b...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\kernel.appcore.dll            SUCCESS   Image Base: 0x74a...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\cryptbase.dll                 SUCCESS   Image Base: 0x757...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\bcryptprimitives.dll          SUCCESS   Image Base: 0x757...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\propsys.dll                   SUCCESS   Image Base: 0x72a...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\oleaut32.dll                  SUCCESS   Image Base: 0x779...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\clbcatq.dll                   SUCCESS   Image Base: 0x75c...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\profapi.dll                   SUCCESS   Image Base: 0x758...
```

Fig.15.1 Importing dlls



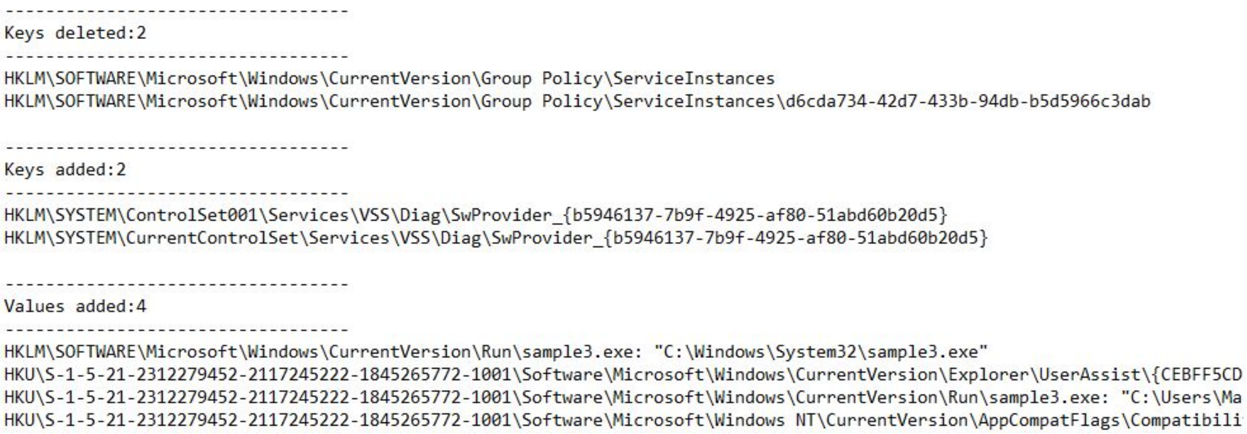
```
Time ...  Process Name   PID   Operation    Path                                              Result    Detail
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\setupapi.dll                  SUCCESS   Image Base: 0x75d...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\cfgmgr32.dll                  SUCCESS   Image Base: 0x75c...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\urlmon.dll                    SUCCESS   Image Base: 0x70b...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\iertutil.dll                  SUCCESS   Image Base: 0x709...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\wininet.dll                   SUCCESS   Image Base: 0x707...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\userenv.dll                   SUCCESS   Image Base: 0x750...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\secur32.dll                   SUCCESS   Image Base: 0x6f6...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\sspicli.dll                   SUCCESS   Image Base: 0x757...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\cryptsp.dll                   SUCCESS   Image Base: 0x753...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\rsaenh.dll                    SUCCESS   Image Base: 0x74e...
8:07:4... sample3.exe    3344  Load Image   C:\Windows\System32\bcrypt.dll                    SUCCESS   Image Base: 0x754...
8:07:5... sample3.exe    3344  Load Image   C:\Windows\System32\srvcli.dll                    SUCCESS   Image Base: 0x755...
8:07:5... sample3.exe    3344  Load Image   C:\Windows\System32\pcacli.dll                    SUCCESS   Image Base: 0x748...
8:07:5... sample3.exe    3344  Load Image   C:\Windows\System32\sfc_os.dll                    SUCCESS   Image Base: 0x6e1...
8:07:5... sample3.exe    3344  Load Image   C:\Windows\System32\devrtl.dll                    SUCCESS   Image Base: 0x6ea...
8:07:5... sample3.exe    3192  Load Image   C:\Users\Malware\Desktop\Practical3\sample3.exe   SUCCESS   Image Base: 0x400...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\ntdll.dll                     SUCCESS   Image Base: 0x77e...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\kernel32.dll                  SUCCESS   Image Base: 0x77c...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\KernelBase.dll                SUCCESS   Image Base: 0x759...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\apphelp.dll                   SUCCESS   Image Base: 0x747...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\advapi32.dll                  SUCCESS   Image Base: 0x75ff...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\msvcrt.dll                    SUCCESS   Image Base: 0x75f...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\sechost.dll                   SUCCESS   Image Base: 0x776...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\rpcrt4.dll                    SUCCESS   Image Base: 0x77d...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\user32.dll                    SUCCESS   Image Base: 0x777...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\gdi32.dll                     SUCCESS   Image Base: 0x77a...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\imm32.dll                     SUCCESS   Image Base: 0x760...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\msctf.dll                     SUCCESS   Image Base: 0x778...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\shell32.dll                   SUCCESS   Image Base: 0x765...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\combase.dll                   SUCCESS   Image Base: 0x761...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\shlwapi.dll                   SUCCESS   Image Base: 0x75c...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\mpr.dll                       SUCCESS   Image Base: 0x6ef...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\ws2_32.dll                    SUCCESS   Image Base: 0x777...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\nsi.dll                       SUCCESS   Image Base: 0x777...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\cmd.exe                       SUCCESS   Image Base: 0x420...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\vmhgfs.dll                    SUCCESS   Image Base: 0x6eb...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\version.dll                   SUCCESS   Image Base: 0x6f4...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\drprov.dll                    SUCCESS   Image Base: 0x729...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\winsta.dll                    SUCCESS   Image Base: 0x74d...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\ntlanman.dll                  SUCCESS   Image Base: 0x6ce...

Showing 87 of 175,794 events (0.049%)     Backed by virtual memory
```

Fig.15.2 Importing dlls



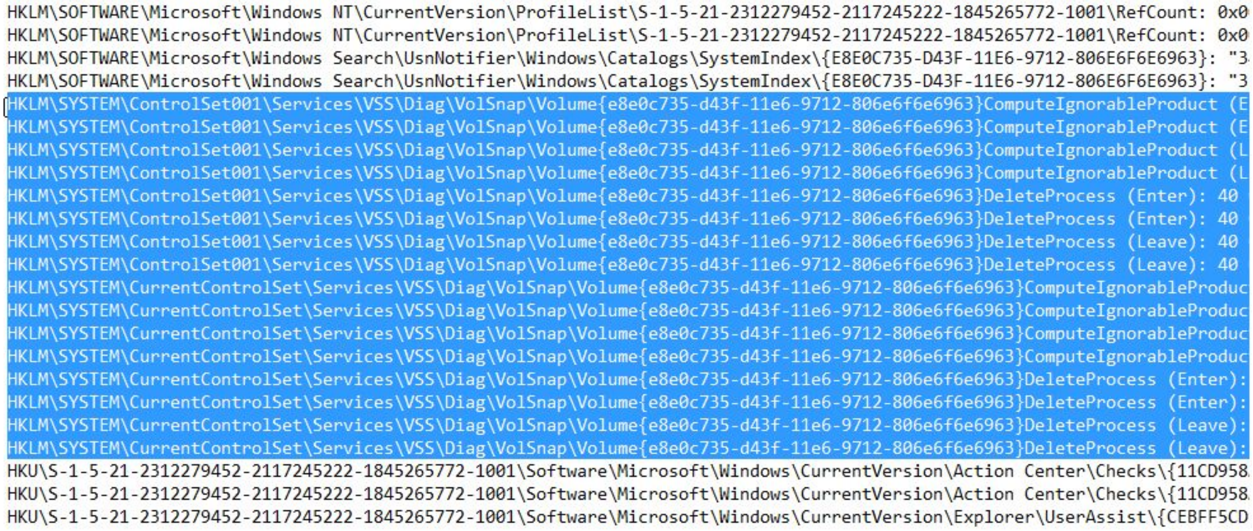
```
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\davclnt.dll                   SUCCESS   Image Base: 0x6ce...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\davhlpr.dll                   SUCCESS   Image Base: 0x729...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\wkscli.dll                    SUCCESS   Image Base: 0x737...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\cscapi.dll                    SUCCESS   Image Base: 0x6d3...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\netutils.dll                  SUCCESS   Image Base: 0x750...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\browcli.dll                   SUCCESS   Image Base: 0x69d...
8:07:5... sample3.exe    3192  Load Image   C:\Windows\System32\srvcli.dll                    SUCCESS   Image Base: 0x755...
```

Fig. 15.3 Importing dlls



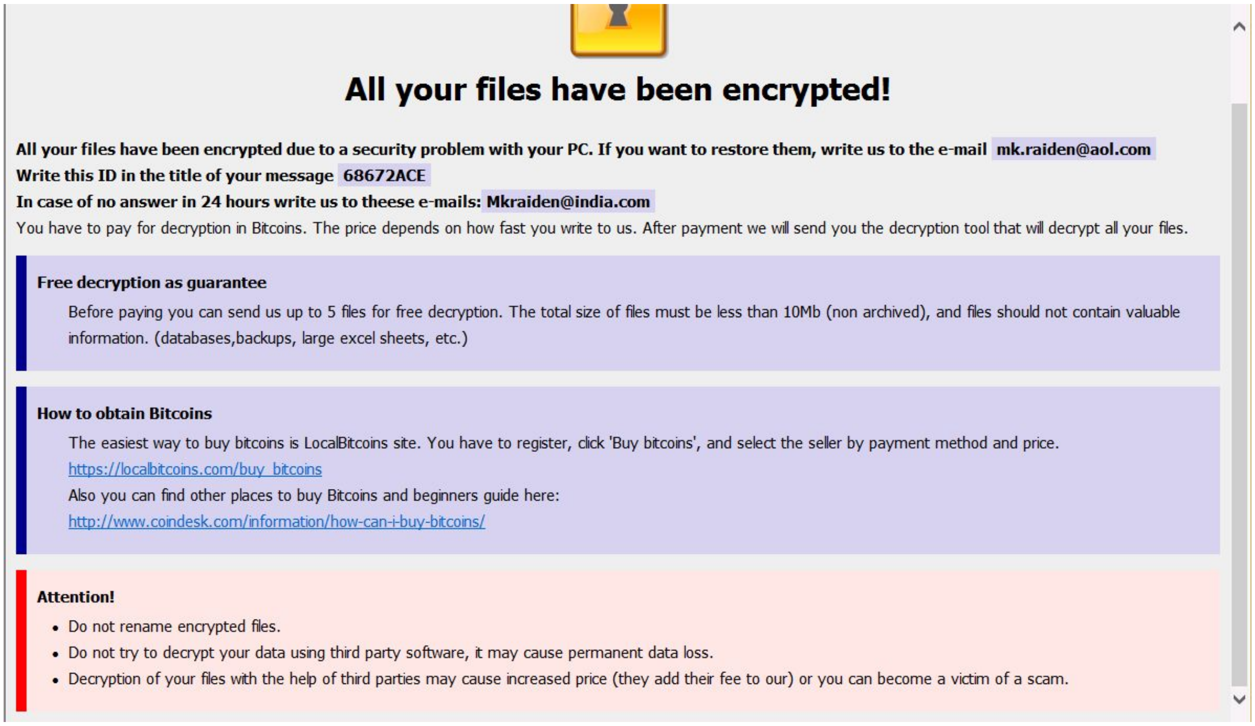
```
----------------------------------
Keys deleted:2
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\d6cda734-42d7-433b-94db-b5d5966c3dab

----------------------------------
Keys added:2
----------------------------------
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
HKLM\SYSTEM\CurrentControlSet\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}

----------------------------------
Values added:4
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\sample3.exe: "C:\Windows\System32\sample3.exe"
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Run\sample3.exe: "C:\Users\Ma
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibili
```

Fig.16.1 Registry updates



```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2312279452-2117245222-1845265772-1001\RefCount: 0x0
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2312279452-2117245222-1845265772-1001\RefCount: 0x0
HKLM\SOFTWARE\Microsoft\Windows Search\UsnNotifier\Windows\Catalogs\SystemIndex\{E8E0C735-D43F-11E6-9712-806E6F6E6963}: "3
HKLM\SOFTWARE\Microsoft\Windows Search\UsnNotifier\Windows\Catalogs\SystemIndex\{E8E0C735-D43F-11E6-9712-806E6F6E6963}: "3
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{e8e0c735-d43f-11e6-9712-806e6f6e6963}ComputeIgnorableProduct (E
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{e8e0c735-d43f-11e6-9712-806e6f6e6963}ComputeIgnorableProduct (E
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{e8e0c735-d43f-11e6-9712-806e6f6e6963}ComputeIgnorableProduct (L
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{e8e0c735-d43f-11e6-9712-806e6f6e6963}ComputeIgnorableProduct (L
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{e8e0c735-d43f-11e6-9712-806e6f6e6963}DeleteProcess (Enter): 40
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{e8e0c735-d43f-11e6-9712-806e6f6e6963}DeleteProcess (Enter): 40
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{e8e0c735-d43f-11e6-9712-806e6f6e6963}DeleteProcess (Leave): 40
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{e8e0c735-d43f-11e6-9712-806e6f6e6963}DeleteProcess (Leave): 40
HKLM\SYSTEM\CurrentControlSet\Services\VSS\Diag\VolSnap\Volume{e8e0c735-d43f-11e6-9712-806e6f6e6963}ComputeIgnorableProduc
HKLM\SYSTEM\CurrentControlSet\Services\VSS\Diag\VolSnap\Volume{e8e0c735-d43f-11e6-9712-806e6f6e6963}ComputeIgnorableProduc
HKLM\SYSTEM\CurrentControlSet\Services\VSS\Diag\VolSnap\Volume{e8e0c735-d43f-11e6-9712-806e6f6e6963}ComputeIgnorableProduc
HKLM\SYSTEM\CurrentControlSet\Services\VSS\Diag\VolSnap\Volume{e8e0c735-d43f-11e6-9712-806e6f6e6963}ComputeIgnorableProduc
HKLM\SYSTEM\CurrentControlSet\Services\VSS\Diag\VolSnap\Volume{e8e0c735-d43f-11e6-9712-806e6f6e6963}DeleteProcess (Enter):
HKLM\SYSTEM\CurrentControlSet\Services\VSS\Diag\VolSnap\Volume{e8e0c735-d43f-11e6-9712-806e6f6e6963}DeleteProcess (Enter):
HKLM\SYSTEM\CurrentControlSet\Services\VSS\Diag\VolSnap\Volume{e8e0c735-d43f-11e6-9712-806e6f6e6963}DeleteProcess (Leave):
HKLM\SYSTEM\CurrentControlSet\Services\VSS\Diag\VolSnap\Volume{e8e0c735-d43f-11e6-9712-806e6f6e6963}DeleteProcess (Leave):
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{11CD958
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{11CD958
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD
```

Fig.16.2 Registry updates



All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail mk.raiden@aol.com
Write this ID in the title of your message 68672ACE
In case of no answer in 24 hours write us to theese e-mails: Mkraiden@india.com
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 10Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

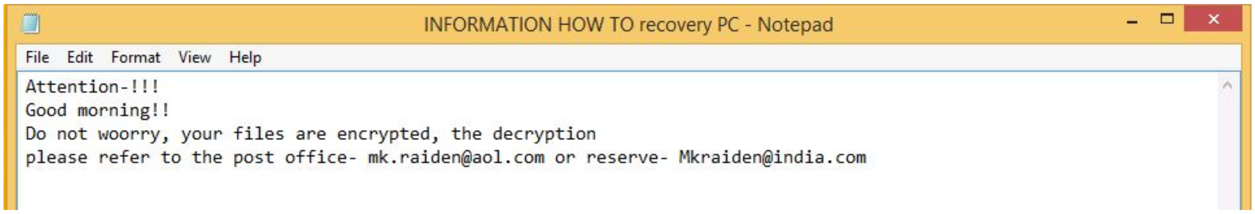
How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!

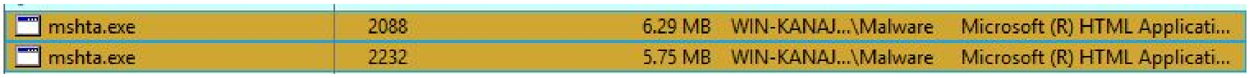
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Fig.17 Page after encryption


INFORMATION HOW TO recovery PC - Notepad
File Edit Format View Help

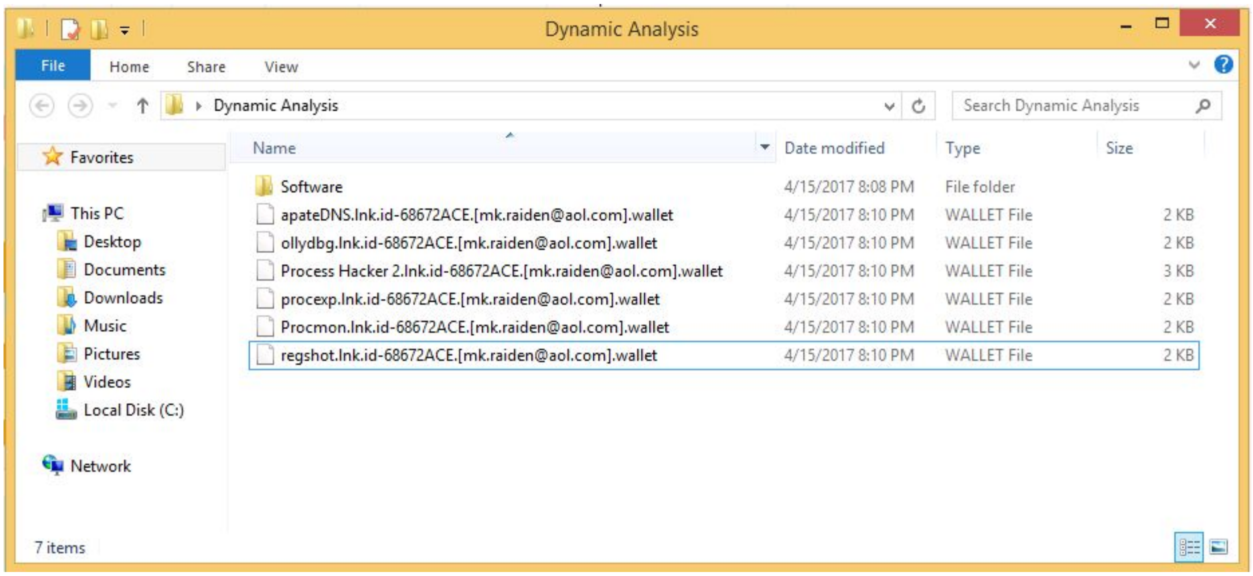
```
Attention-!!!
Good morning!!
Do not woorry, your files are encrypted, the decryption
please refer to the post office- mk.raiden@aol.com or reserve- Mkraiden@india.com
```

Fig.18 Text file created



mshta.exe	2088	6.29 MB	WIN-KANAJ...\Malware	Microsoft (R) HTML Applicati...
mshta.exe	2232	5.75 MB	WIN-KANAJ...\Malware	Microsoft (R) HTML Applicati...

Fig.19 Process mshta spawned



Name	Date modified	Type	Size
Software	4/15/2017 8:08 PM	File folder	
apateDNS.lnk.id-68672ACE.[mk.raiden@aol.com].wallet	4/15/2017 8:10 PM	WALLET File	2 KB
ollydbg.lnk.id-68672ACE.[mk.raiden@aol.com].wallet	4/15/2017 8:10 PM	WALLET File	2 KB
Process Hacker 2.lnk.id-68672ACE.[mk.raiden@aol.com].wallet	4/15/2017 8:10 PM	WALLET File	3 KB
procexp.lnk.id-68672ACE.[mk.raiden@aol.com].wallet	4/15/2017 8:10 PM	WALLET File	2 KB
Procmon.lnk.id-68672ACE.[mk.raiden@aol.com].wallet	4/15/2017 8:10 PM	WALLET File	2 KB
regshot.lnk.id-68672ACE.[mk.raiden@aol.com].wallet	4/15/2017 8:10 PM	WALLET File	2 KB

Fig.20 New encrypted .wallet files created

Advanced Static and Dynamic Analysis

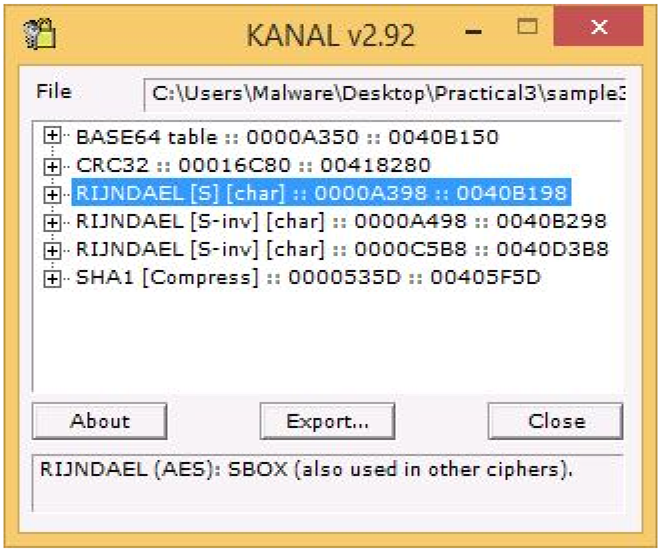
The malware sample employs a number of cryptographic techniques for its encryption. We can analyse this using the Krypto ANAlyzer plugin for PEiD which examines constants associated with certain cryptographic schemes present in the file. The KANAL analysis shows us that the malware predominantly uses the AES encryption scheme and tells us that it is being referenced at the address 40B198. The results are presented below.

The program attempts to build its own IAT dynamically. We observe this using Ollydbg referencing the locations where "LoadlibraryA" and "GetProcAddress" are called. By putting a breakpoint on the function call and examining the registers, we see that each call to "LoadLibraryA" has a dll as an argument and each call to "GetProcAddress" has a corresponding process as an argument. These functions build the IAT which is used later by the program as required. The results are shown below.

Using IDA's proximity view, we see that there are a large number of functions differing only be a constant address which look almost the same in functionality. These functions represent the imports and each one corresponds to a different function. These functions are all called by the sub_402880 which is the main driver function of the program.

Sub_402880 also calls sub_403960. By examining the arguments passed to sub_403960 using Ollydbg, we see that this function traverses through the file system directory reading the contents of each and every file it selects. The arguments passed differ in every iteration of the program being run thereby suggesting that the selection order is random. Once a file is selected, the function proceeds to read its contents performing some manipulation on them. It is assumed that this is where the encryption occurs.

We present 3 functions out of the IAT that are ef particular interest. “Readfile” is used to read the contents of each file before encryption, “Deletefile” is used after the encryption process to remove the original file. And finally “Writefile” writes out the encrypted content to the new file. We can observe the structure of each file by opening it in an editor. While most files display an Oriental character set, some are still visible in ASCII format. We observe that each “.wallet” file begins with significantly different data. This is assumed to be the original encrypted data of each file. We can further observe this by viewing 2 separate files containing the same data. After the encrypted data, every file ends with a footer containing 5 different sections of data. The 1st section is the same for every file and is a particular ASCII character set. This is followed by the 2nd section which is the file name followed by a string which starts with 134MMK. This string is also the same for every single file and is mostly an identifier used by the malware author whose ID seems to be “mk.raiden”. The 3rd section is different for every file and can potentially be a key used in the encryption process. The 4th section seems to be some form of directory identifier as it is the same for files from the same folder however different for files from other folders. The 5th and final section consists of a file identifier and is probably a serial number. It is different for every file yet only consists of 1 or 2 characters as observed. The file structures are shown below.
Before the call to “Writefile”, on analysing the arguments passed through register EAX, we observe that it contains the footer content to be written out to the file. This footer content further confirms the aforementioned statements.

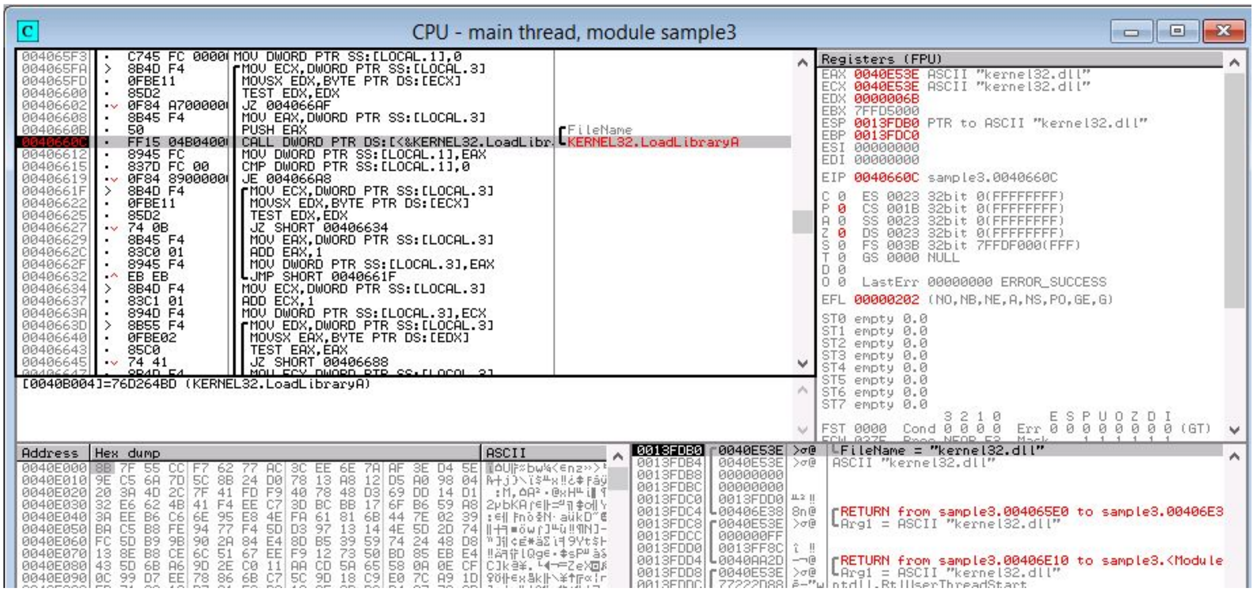


File C:\Users\Malware\Desktop\Practical3\sample3

```
BASE64 table :: 0000A350 :: 0040B150
CRC32 :: 00016C80 :: 00418280
RIJNDAEL [S] [char] :: 0000A398 :: 0040B198
RIJNDAEL [S-inv] [char] :: 0000A498 :: 0040B298
RIJNDAEL [S-inv] [char] :: 0000C5B8 :: 0040D3B8
SHA1 [Compress] :: 0000535D :: 00405F5D
```

RIJNDAEL (AES): SBOX (also used in other ciphers).

Fig.21 KANAL



CPU - main thread, module sample3

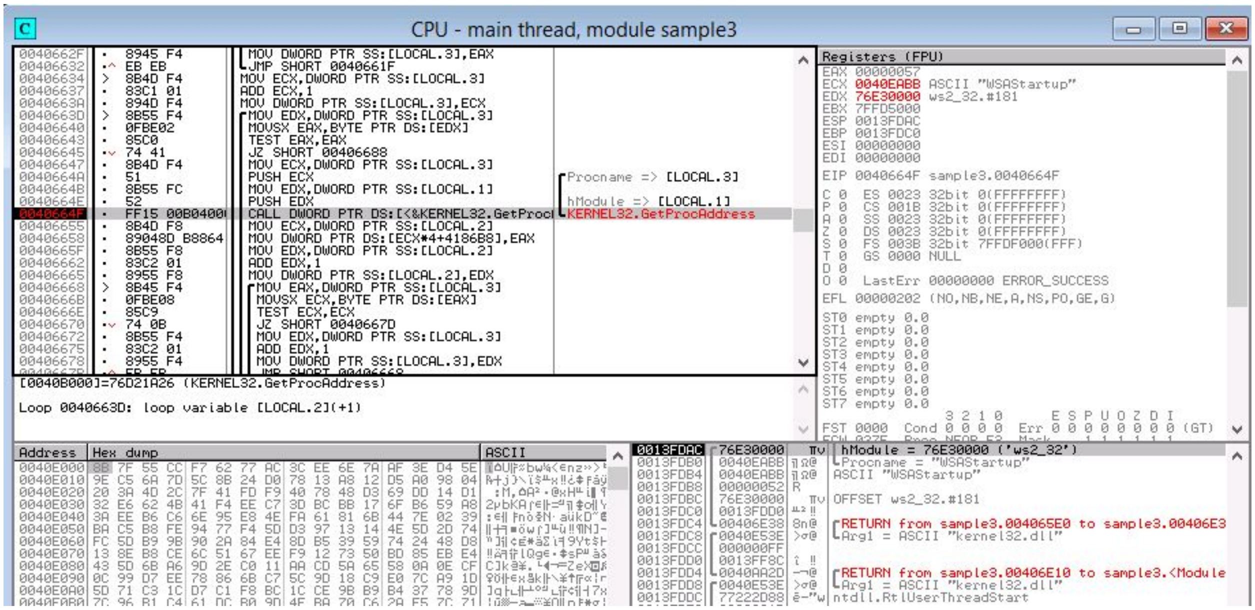
```
004065F3  .  C745 FC 0000  MOV DWORD PTR SS:[LOCAL.1],0
004065FA  >  8B4D F4       MOV ECX,DWORD PTR SS:[LOCAL.3]
004065FD  .  0FBE11        MOVSX EDX,BYTE PTR DS:[ECX]
00406600  .  85D2          TEST EDX,EDX
00406602  .v 0F84 A700000  JZ 004066AF
00406608  .  8B45 F4       MOV EAX,DWORD PTR SS:[LOCAL.3]
0040660B  .  50            PUSH EAX                               FileName
0040660C  .  FF15 04B0400  CALL DWORD PTR DS:[<&KERNEL32.LoadLibr  KERNEL32.LoadLibraryA
00406612  .  8945 FC       MOV DWORD PTR SS:[LOCAL.1],EAX
00406615  .  837D FC 00    CMP DWORD PTR SS:[LOCAL.1],0
00406619  .v 0F84 8900000  JE 004066A8
0040661F  >  8B4D F4        MOV ECX,DWORD PTR SS:[LOCAL.3]
00406622  .  0FBE11         MOVSX EDX,BYTE PTR DS:[ECX]
00406625  .  85D2           TEST EDX,EDX
00406627  .v 74 0B          JZ SHORT 00406634
00406629  .  8B45 F4        MOV EAX,DWORD PTR SS:[LOCAL.3]
0040662C  .  83C0 01        ADD EAX,1
0040662F  .  8945 F4        MOV DWORD PTR SS:[LOCAL.3],EAX
00406632  .^ EB EB          JMP SHORT 0040661F
00406634  >  8B4D F4       MOV ECX,DWORD PTR SS:[LOCAL.3]
00406637  .  83C1 01       ADD ECX,1
0040663A  .  894D F4       MOV DWORD PTR SS:[LOCAL.3],ECX
0040663D  >  8B55 F4        MOV EDX,DWORD PTR SS:[LOCAL.3]
00406640  .  0FBE02         MOVSX EAX,BYTE PTR DS:[EDX]
00406643  .  85C0           TEST EAX,EAX
00406645  .v 74 41          JZ SHORT 00406688
[0040B004]=76D264BD (KERNEL32.LoadLibraryA)
```

```
Registers (FPU)
EAX 0040E53E ASCII "kernel32.dll"
ECX 0040E53E ASCII "kernel32.dll"
EDX 0000006B
EBX 7FFD5000
ESP 0013FDB0 PTR to ASCII "kernel32.dll"
EBP 0013FDC0
ESI 00000000
EDI 00000000

EIP 0040660C sample3.0040660C

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr 00000000 ERROR_SUCCESS

EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0 (GT)
```

```
Address   Hex dump
0040E000  8B 7F 55 CC F7 62 77 AC 3C EE 6E 7A AF 3E D4 5E
0040E010  9E C5 6A 7D 5C 8B 24 D0 78 13 A8 12 D5 A0 98 04
0040E020  20 3A 4D 2C 7F 41 FD F9 40 78 48 D3 69 DD 14 D1
0040E030  32 E6 62 4B 41 F4 EE C7 3D BC BB 17 6F B6 59 A8
0040E040  3A EE B6 C6 6E 95 E8 4E FA 61 81 6B 44 7E 02 39
0040E050  BA C5 B8 FE 94 77 F4 5D D3 97 13 14 4E 5D 2D 74
0040E060  FC 5D B9 9B 90 2A 84 E4 8D B5 39 59 74 24 48 D8
0040E070  13 8E B8 CE 6C 51 67 EE F9 12 73 50 BD 85 EB E4
0040E080  43 5D 6B A6 9D 2E C0 11 AA CD 5A 65 58 0A 0E CF
0040E090  0C 99 D7 EE 78 86 6B C7 5C 9D 18 C9 E0 7C A9 1D
```

```
0013FDB0  0040E53E  >σ@  FileName = "kernel32.dll"
0013FDB4  0040E53E  >σ@  ASCII "kernel32.dll"
0013FDB8  00000000
0013FDBC  00000000
0013FDC0  0013FDD0
0013FDC4  00406E38  8n@  RETURN from sample3.004065E0 to sample3.00406E3
0013FDC8  0040E53E  >σ@  Arg1 = ASCII "kernel32.dll"
0013FDCC  000000FF
0013FDD0  0013FF8C
0013FDD4  0040AA2D       RETURN from sample3.00406E10 to sample3.<Module
0013FDD8  0040E53E  >σ@  Arg1 = ASCII "kernel32.dll"
0013FDDC  77222D88       ntdll.RtlUserThreadStart
```

Fig.22 LoadLibraryA



CPU - main thread, module sample3

```
0040662F  .  8945 F4        MOV DWORD PTR SS:[LOCAL.3],EAX
00406632  .^ EB EB          JMP SHORT 0040661F
00406634  >  8B4D F4       MOV ECX,DWORD PTR SS:[LOCAL.3]
00406637  .  83C1 01       ADD ECX,1
0040663A  .  894D F4       MOV DWORD PTR SS:[LOCAL.3],ECX
0040663D  >  8B55 F4        MOV EDX,DWORD PTR SS:[LOCAL.3]
00406640  .  0FBE02         MOVSX EAX,BYTE PTR DS:[EDX]
00406643  .  85C0           TEST EAX,EAX
00406645  .v 74 41          JZ SHORT 00406688
00406647  .  8B4D F4        MOV ECX,DWORD PTR SS:[LOCAL.3]
0040664A  .  51             PUSH ECX                               Procname => [LOCAL.3]
0040664B  .  8B55 FC        MOV EDX,DWORD PTR SS:[LOCAL.1]
0040664E  .  52             PUSH EDX                               hModule => [LOCAL.1]
0040664F  .  FF15 00B0400   CALL DWORD PTR DS:[<&KERNEL32.GetProc  KERNEL32.GetProcAddress
00406655  .  8B4D F8        MOV ECX,DWORD PTR SS:[LOCAL.2]
00406658  .  89048D B8864   MOV DWORD PTR DS:[ECX*4+4186B8],EAX
0040665F  .  8B55 F8        MOV EDX,DWORD PTR SS:[LOCAL.2]
00406662  .  83C2 01        ADD EDX,1
00406665  .  8955 F8        MOV DWORD PTR SS:[LOCAL.2],EDX
00406668  >  8B45 F4         MOV EAX,DWORD PTR SS:[LOCAL.3]
0040666B  .  0FBE08          MOVSX ECX,BYTE PTR DS:[EAX]
0040666E  .  85C9            TEST ECX,ECX
00406670  .v 74 0B           JZ SHORT 0040667D
00406672  .  8B55 F4         MOV EDX,DWORD PTR SS:[LOCAL.3]
00406675  .  83C2 01         ADD EDX,1
00406678  .  8955 F4         MOV DWORD PTR SS:[LOCAL.3],EDX
[0040B000]=76D21A26 (KERNEL32.GetProcAddress)

Loop 0040663D: loop variable [LOCAL.2](+1)
```

```
Registers (FPU)
EAX 00000057
ECX 0040EABB ASCII "WSAStartup"
EDX 76E30000 ws2_32.#181
EBX 7FFD5000
ESP 0013FDAC
EBP 0013FDC0
ESI 00000000
EDI 00000000

EIP 0040664F sample3.0040664F

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr 00000000 ERROR_SUCCESS

EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0 (GT)
```

```
Address   Hex dump
0040E000  8B 7F 55 CC F7 62 77 AC 3C EE 6E 7A AF 3E D4 5E
0040E010  9E C5 6A 7D 5C 8B 24 D0 78 13 A8 12 D5 A0 98 04
0040E020  20 3A 4D 2C 7F 41 FD F9 40 78 48 D3 69 DD 14 D1
0040E030  32 E6 62 4B 41 F4 EE C7 3D BC BB 17 6F B6 59 A8
0040E040  3A EE B6 C6 6E 95 E8 4E FA 61 81 6B 44 7E 02 39
0040E050  BA C5 B8 FE 94 77 F4 5D D3 97 13 14 4E 5D 2D 74
0040E060  FC 5D B9 9B 90 2A 84 E4 8D B5 39 59 74 24 48 D8
0040E070  13 8E B8 CE 6C 51 67 EE F9 12 73 50 BD 85 EB E4
0040E080  43 5D 6B A6 9D 2E C0 11 AA CD 5A 65 58 0A 0E CF
0040E090  0C 99 D7 EE 78 86 6B C7 5C 9D 18 C9 E0 7C A9 1D
0040E0A0  5D 71 C3 1C D7 C1 F8 BC 1C CE 9B B9 B4 37 78 9D
```

```
0013FDAC  76E30000   πv  hModule = 76E30000 ('ws2_32')
0013FDB0  0040EABB  ╗Ω@  Procname = "WSAStartup"
0013FDB4  0040EABB  ╗Ω@  ASCII "WSAStartup"
0013FDB8  00000052  R
0013FDBC  76E30000   πv  OFFSET ws2_32.#181
0013FDC0  0013FDD0
0013FDC4  00406E38  8n@  RETURN from sample3.004065E0 to sample3.00406E3
0013FDC8  0040E53E  >σ@  Arg1 = ASCII "kernel32.dll"
0013FDCC  000000FF
0013FDD0  0013FF8C
0013FDD4  0040AA2D       RETURN from sample3.00406E10 to sample3.<Module
0013FDD8  0040E53E  >σ@  Arg1 = ASCII "kernel32.dll"
0013FDDC  77222D88       ntdll.RtlUserThreadStart
```

Fig.23 GetProcAddress

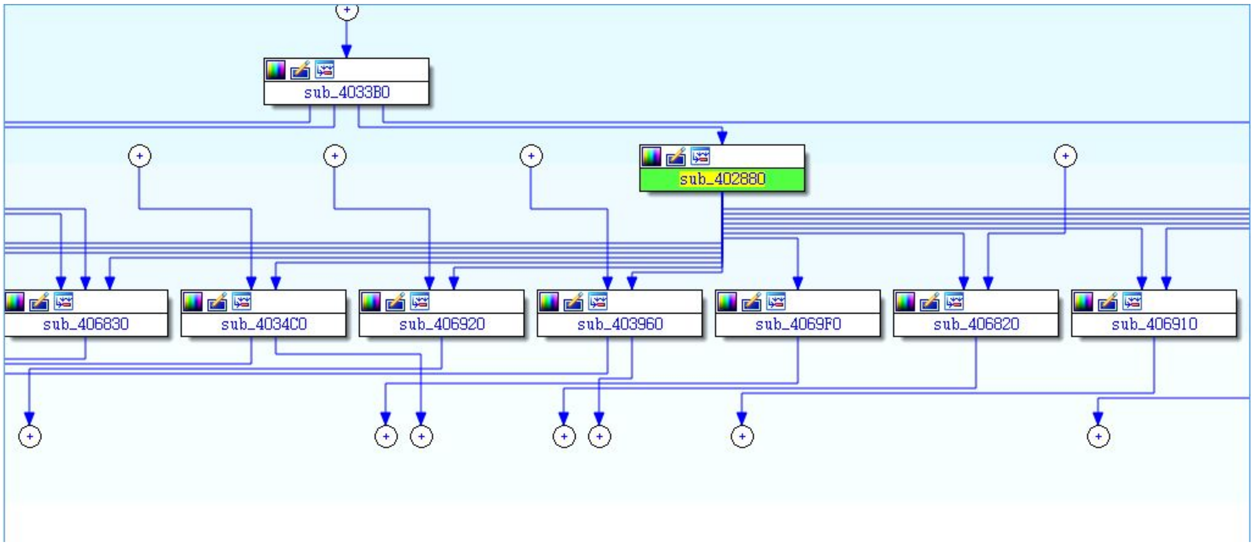
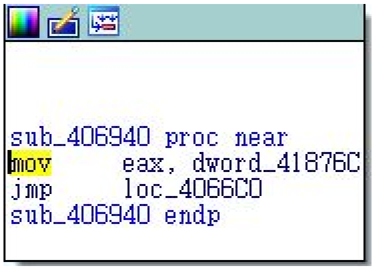
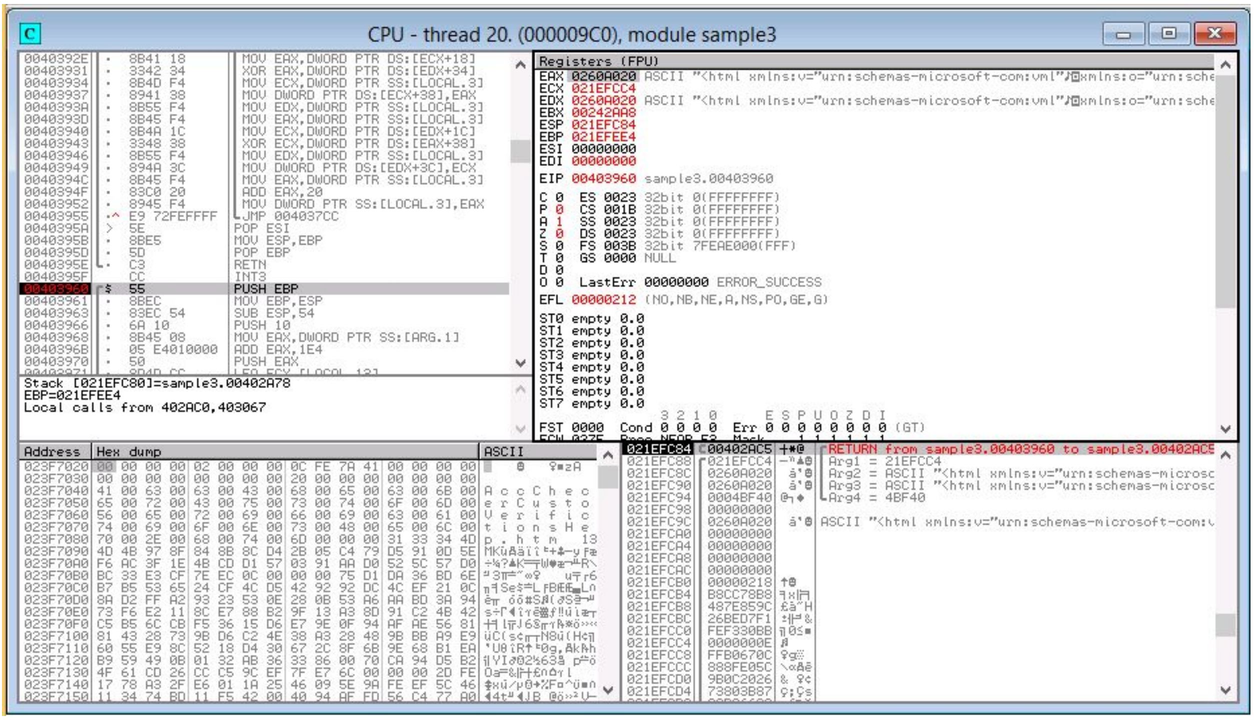


Fig.24 IAT referened



```
sub_406940 proc near
mov     eax, dword_41876C
jmp     loc_4066C0
sub_406940 endp
```

Fig.25 Import Content



CPU - thread 20. (000009C0), module sample3

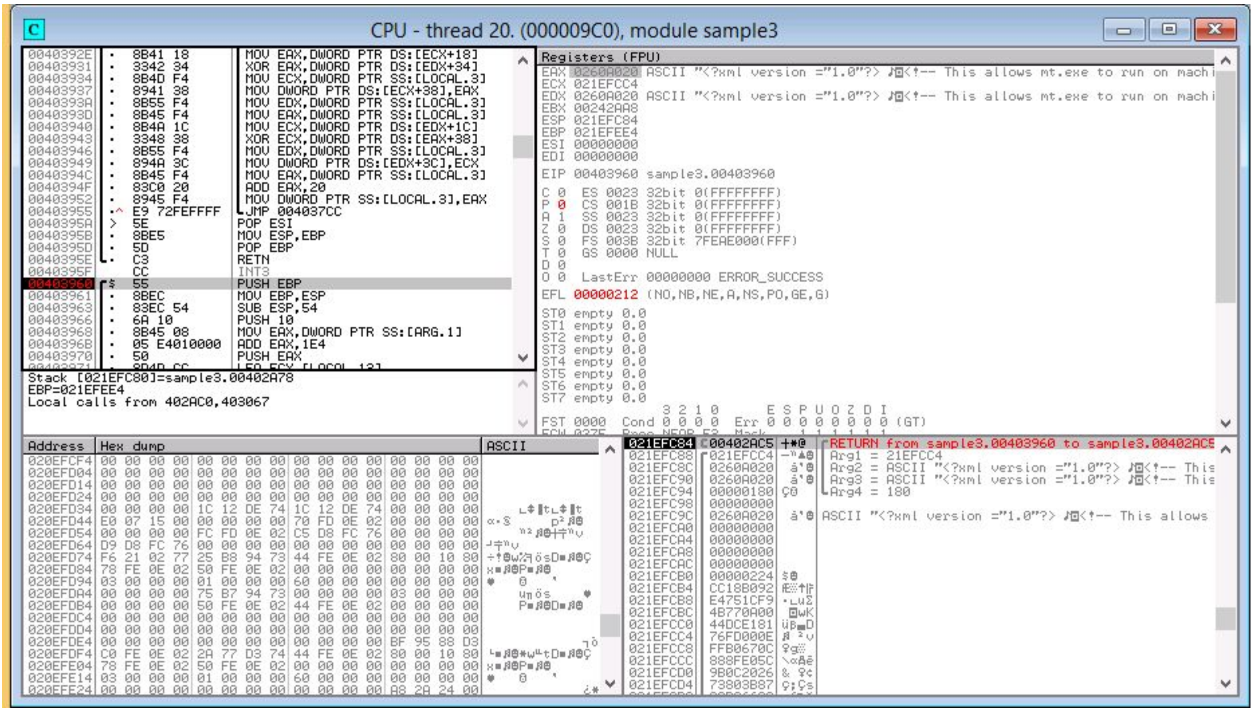
```
0040392E  .  8B41 18        MOV EAX,DWORD PTR DS:[ECX+18]
00403931  .  3342 34        XOR EAX,DWORD PTR DS:[EDX+34]
00403934  .  8B4D F4        MOV ECX,DWORD PTR SS:[LOCAL.3]
00403937  .  8941 38        MOV DWORD PTR DS:[ECX+38],EAX
0040393A  .  8B55 F4        MOV EDX,DWORD PTR SS:[LOCAL.3]
0040393D  .  8B45 F4        MOV EAX,DWORD PTR SS:[LOCAL.3]
00403940  .  8B4A 1C        MOV ECX,DWORD PTR DS:[EDX+1C]
00403943  .  3348 38        XOR ECX,DWORD PTR DS:[EAX+38]
00403946  .  8B55 F4        MOV EDX,DWORD PTR SS:[LOCAL.3]
00403949  .  894A 3C        MOV DWORD PTR DS:[EDX+3C],ECX
0040394C  .  8B45 F4        MOV EAX,DWORD PTR SS:[LOCAL.3]
0040394F  .  83C0 20        ADD EAX,20
00403952  .  8945 F4        MOV DWORD PTR SS:[LOCAL.3],EAX
00403955  .^ E9 72FEFFFF    JMP 004037CC
0040395A  >  5E             POP ESI
0040395B  .  8BE5           MOV ESP,EBP
0040395D  .  5D             POP EBP
0040395E  .  C3             RETN
0040395F     CC             INT3
00403960  $  55             PUSH EBP
00403961  .  8BEC           MOV EBP,ESP
00403963  .  83EC 54        SUB ESP,54
00403966  .  6A 10          PUSH 10
00403968  .  8B45 08        MOV EAX,DWORD PTR SS:[ARG.1]
0040396B  .  05 E4010000    ADD EAX,1E4
00403970  .  50             PUSH EAX

Stack [021EFC80]=sample3.00402A78
EBP=021EFEE4
Local calls from 402AC0,403067
```

```
Registers (FPU)
EAX 0260A020 ASCII "<html xmlns:v="urn:schemas-microsoft-com:vml"♪◘xmlns:o="urn:sche
ECX 021EFCC4
EDX 0260A020 ASCII "<html xmlns:v="urn:schemas-microsoft-com:vml"♪◘xmlns:o="urn:sche
EBX 00242AA8
ESP 021EFC84
EBP 021EFEE4
ESI 00000000
EDI 00000000

EIP 00403960 sample3.00403960

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 1  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FEAE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr 00000000 ERROR_SUCCESS

EFL 00000212 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0 (GT)
```

```
Address   Hex dump                                         ASCII
023F7020  00 00 00 00 02 00 00 00 0C FE 7A 41 00 00 00 00     ☻   ♀■zA
023F7030  00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00
023F7040  41 00 63 00 63 00 43 00 68 00 65 00 63 00 6B 00  A c c C h e c
023F7050  65 00 72 00 43 00 75 00 73 00 74 00 6F 00 6D 00  e r C u s t o
023F7060  56 00 65 00 72 00 69 00 66 00 69 00 63 00 61 00  V e r i f i c
023F7070  74 00 69 00 6F 00 6E 00 73 00 48 00 65 00 6C 00  t i o n s H e
023F7080  70 00 2E 00 68 00 74 00 6D 00 00 00 31 33 34 4D  p . h t m   13
023F7090  4D 4B 97 8F 84 8B 8C D4 2B 05 C4 79 D5 91 0D 5E  MKùÅäïî╘+♣─y╒æ
023F70A0  F6 AC 3F 1E 4B CD D1 57 03 91 AA D0 52 5C 57 D0  ÷¼?▲K═╤W♥æ¬╨R\
023F70B0  BC 33 E3 CF 7E EC 0C 00 00 00 75 D1 DA 36 BD 6E  ╝3π╧~∞♀   u╤┌6
023F70C0  B7 B5 53 65 24 CF 4C D5 42 92 92 DC 4C EF 21 0C  ╖╡Se$╧L╒BÆÆ▄L∩
023F70D0  8A D2 FF A2 93 23 53 0E 28 0B 53 A6 AA BD 3A 94  è╥ óô#S♫(♂Sª¬╜
023F70E0  73 F6 E2 11 8C E7 88 B2 9F 13 A3 8D 91 C2 4B 42  s÷Γ◄îτê▓ƒ‼úìæ┬
023F70F0  C5 B5 6C CB F5 36 15 D6 E7 9E 0F 94 AF AE 56 81  ┼╡l╦ⁿ6§╓τ₧☼ö»«
023F7100  81 43 28 73 9B D6 C2 4E 38 A3 28 48 9B BB A9 E9  üC(s¢╓┬N8ú(H¢╗
023F7110  60 55 E9 8C 52 18 D4 30 67 2C 8F 6B 9E 68 B1 EA  `UΘîR↑╘0g,Åk₧h
023F7120  B9 59 49 0B 01 32 AB 36 33 86 00 70 CA 94 D5 B2  ╣YI♂☺2½63å p╩ö
023F7130  4F 61 CD 26 CC C5 9C EF 7F E7 6C 00 00 00 2D FE  Oa═&╠┼£∩⌂τl
023F7140  17 78 A3 2F E6 01 1A 25 46 09 5E 9A FE EF 5C 46  ↨xú/µ☺→%F○^Ü■∩
```

```
021EFC84  00402AC5  +*@   RETURN from sample3.00403960 to sample3.00402AC5
021EFC88  021EFCC4  ─ⁿ▲☻  Arg1 = 21EFCC4
021EFC8C  0260A020   á'☻  Arg2 = ASCII "<html xmlns:v="urn:schemas-microsc
021EFC90  0260A020   á'☻  Arg3 = ASCII "<html xmlns:v="urn:schemas-microsc
021EFC94  0004BF40  @┐♦   Arg4 = 4BF40
021EFC98  00000000
021EFC9C  0260A020   á'☻  ASCII "<html xmlns:v="urn:schemas-microsoft-com:v
021EFCA0  00000000
021EFCA4  00000000
021EFCA8  00000000
021EFCAC  00000000
021EFCB0  00000218  ↑☻
021EFCB4  B8CC78B8  ╕x╠╕
021EFCB8  487E859C  £à~H
021EFCBC  26BED7F1  ±╫╛&
021EFCC0  FEF330BB  ╗0≤■
021EFCC4  0000000E  ♫
021EFCC8  FFB0670C  ♀g░
021EFCCC  888FE05C  \αÅê
021EFCD0  9B0C2026  & ♀¢
021EFCD4  73803B87  ç;Çs
```

Fig.26.1 sub_403960



CPU - thread 20. (000009C0), module sample3

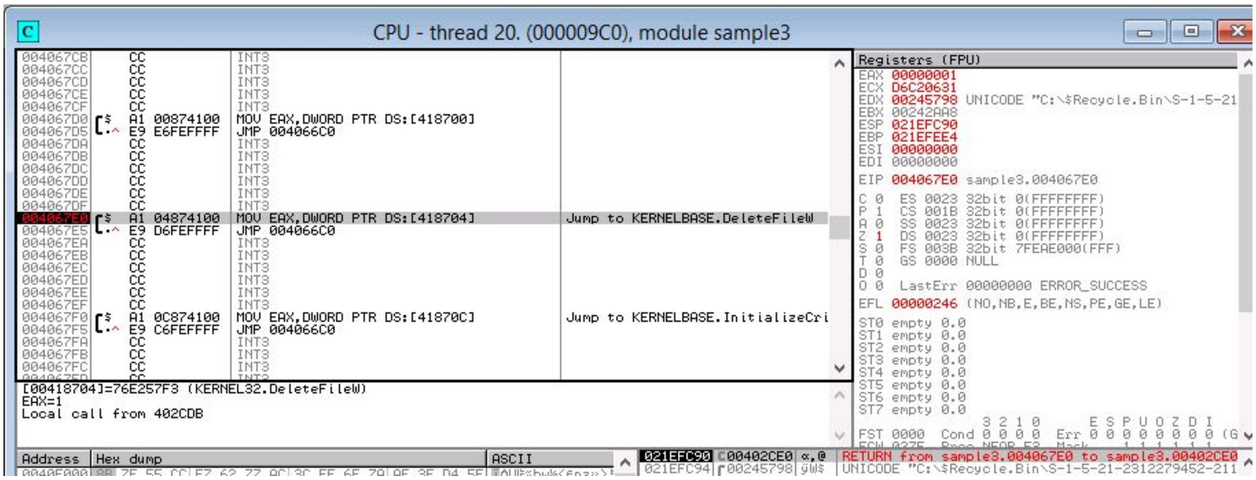
```
0040392E  .  8B41 18        MOV EAX,DWORD PTR DS:[ECX+18]
00403931  .  3342 34        XOR EAX,DWORD PTR DS:[EDX+34]
00403934  .  8B4D F4        MOV ECX,DWORD PTR SS:[LOCAL.3]
00403937  .  8941 38        MOV DWORD PTR DS:[ECX+38],EAX
0040393A  .  8B55 F4        MOV EDX,DWORD PTR SS:[LOCAL.3]
0040393D  .  8B45 F4        MOV EAX,DWORD PTR SS:[LOCAL.3]
00403940  .  8B4A 1C        MOV ECX,DWORD PTR DS:[EDX+1C]
00403943  .  3348 38        XOR ECX,DWORD PTR DS:[EAX+38]
00403946  .  8B55 F4        MOV EDX,DWORD PTR SS:[LOCAL.3]
00403949  .  894A 3C        MOV DWORD PTR DS:[EDX+3C],ECX
0040394C  .  8B45 F4        MOV EAX,DWORD PTR SS:[LOCAL.3]
0040394F  .  83C0 20        ADD EAX,20
00403952  .  8945 F4        MOV DWORD PTR SS:[LOCAL.3],EAX
00403955  .^ E9 72FEFFFF    JMP 004037CC
0040395A  >  5E             POP ESI
0040395B  .  8BE5           MOV ESP,EBP
0040395D  .  5D             POP EBP
0040395E  .  C3             RETN
0040395F     CC             INT3
00403960  $  55             PUSH EBP
00403961  .  8BEC           MOV EBP,ESP
00403963  .  83EC 54        SUB ESP,54
00403966  .  6A 10          PUSH 10
00403968  .  8B45 08        MOV EAX,DWORD PTR SS:[ARG.1]
0040396B  .  05 E4010000    ADD EAX,1E4
00403970  .  50             PUSH EAX

Stack [021EFC80]=sample3.00402A78
EBP=021EFEE4
Local calls from 402AC0,403067
```

```
Registers (FPU)
EAX 0260A020 ASCII "<?xml version ="1.0"?> ♪◘<!-- This allows mt.exe to run on machi
ECX 021EFCC4
EDX 0260A020 ASCII "<?xml version ="1.0"?> ♪◘<!-- This allows mt.exe to run on machi
EBX 00242AA8
ESP 021EFC84
EBP 021EFEE4
ESI 00000000
EDI 00000000

EIP 00403960 sample3.00403960

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 1  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FEAE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr 00000000 ERROR_SUCCESS

EFL 00000212 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0 (GT)
```

```
Address   Hex dump                                         ASCII
020EFCF4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
020EFD04  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
020EFD14  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
020EFD24  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
020EFD34  00 00 00 00 1C 12 DE 74 1C 12 DE 74 00 00 00 00      ∟↕▐t∟↕▐t
020EFD44  E0 07 15 00 00 00 00 00 70 FD 0E 02 00 00 00 00  α•§     p²♫☻
020EFD54  00 00 00 00 FC FD 0E 02 C5 D8 FC 76 00 00 00 00      ⁿ²♫☻┼╪ⁿv
020EFD64  D9 D8 FC 76 00 00 00 00 00 00 00 00 00 00 00 00  ┘╪ⁿv
020EFD74  F6 21 02 77 25 B8 94 73 44 FE 0E 02 80 00 10 80  ÷!☻w%╕ösD■♫☻Ç
020EFD84  78 FE 0E 02 50 FE 0E 02 00 00 00 00 00 00 00 00  x■♫☻P■♫☻
020EFD94  03 00 00 00 01 00 00 00 60 00 00 00 00 00 00 00  ♥   ☺   `
020EFDA4  00 00 00 00 75 B7 94 73 00 00 00 00 03 00 00 00      u╖ös    ♥
020EFDB4  00 00 00 00 50 FE 0E 02 44 FE 0E 02 00 00 00 00      P■♫☻D■♫☻
020EFDC4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
020EFDD4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
020EFDE4  00 00 00 00 00 00 00 00 00 00 00 00 BF 95 88 D3              ┐ò
020EFDF4  C0 FE 0E 02 2A 77 D3 74 44 FE 0E 02 80 00 10 80  └■♫☻*w╙tD■♫☻Ç
020EFE04  78 FE 0E 02 50 FE 0E 02 00 00 00 00 00 00 00 00  x■♫☻P■♫☻
020EFE14  03 00 00 00 01 00 00 00 60 00 00 00 00 00 00 00  ♥   ☺   `
```

```
021EFC84  00402AC5  +*@   RETURN from sample3.00403960 to sample3.00402AC5
021EFC88  021EFCC4  ─ⁿ▲☻  Arg1 = 21EFCC4
021EFC8C  0260A020   á'☻  Arg2 = ASCII "<?xml version ="1.0"?> ♪◘<!-- This
021EFC90  0260A020   á'☻  Arg3 = ASCII "<?xml version ="1.0"?> ♪◘<!-- This
021EFC94  00000180  Ç☺    Arg4 = 180
021EFC98  00000000
021EFC9C  0260A020   á'☻  ASCII "<?xml version ="1.0"?> ♪◘<!-- This allows
021EFCA0  00000000
021EFCA4  00000000
021EFCA8  00000000
021EFCAC  00000000
021EFCB0  00000224  $☻
021EFCB4  CC18B092  Æ░↑╠
021EFCB8  E4751CF9  ·∟uΣ
021EFCBC  4B770A00   ◙wK
021EFCC0  44DCE181  üß▄D
021EFCC4  76FD000E  ♫ ²v
021EFCC8  FFB0670C  ♀g░
021EFCCC  888FE05C  \αÅê
021EFCD0  9B0C2026  & ♀¢
021EFCD4  73803B87  ç;Çs
```

Fig.26.2 sub_403960



CPU - thread 20. (000009C0), module sample3

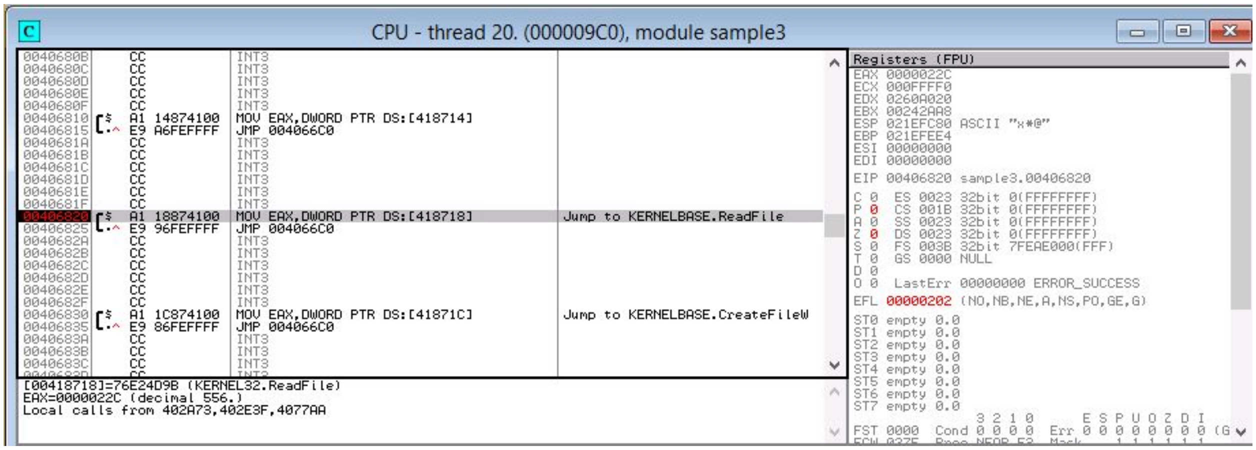
```
004067CB     CC            INT3
004067CC     CC            INT3
004067CD     CC            INT3
004067CE     CC            INT3
004067CF     CC            INT3
004067D0  $  A1 00874100   MOV EAX,DWORD PTR DS:[418700]
004067D5  .^ E9 E6FEFFFF   JMP 004066C0
004067DA     CC            INT3
004067DB     CC            INT3
004067DC     CC            INT3
004067DD     CC            INT3
004067DE     CC            INT3
004067DF     CC            INT3
004067E0  $  A1 04874100   MOV EAX,DWORD PTR DS:[418704]            Jump to KERNELBASE.DeleteFileW
004067E5  .^ E9 D6FEFFFF   JMP 004066C0
004067EA     CC            INT3
004067EB     CC            INT3
004067EC     CC            INT3
004067ED     CC            INT3
004067EE     CC            INT3
004067EF     CC            INT3
004067F0  $  A1 0C874100   MOV EAX,DWORD PTR DS:[41870C]            Jump to KERNELBASE.InitializeCri
004067F5  .^ E9 C6FEFFFF   JMP 004066C0
004067FA     CC            INT3
004067FB     CC            INT3
004067FC     CC            INT3
```

```
[00418704]=76E257F3 (KERNEL32.DeleteFileW)
EAX=1
Local call from 402CDB
```

```
Registers (FPU)
EAX 00000001
ECX D6C20631
EDX 00245798 UNICODE "C:\$Recycle.Bin\S-1-5-21
EBX 00242AA8
ESP 021EFC90
EBP 021EFEE4
ESI 00000000
EDI 00000000

EIP 004067E0 sample3.004067E0

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FEAE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr 00000000 ERROR_SUCCESS

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0 (G
```

```
Address   Hex dump                                ASCII
021EFC90  00402CE0  α,@   RETURN from sample3.004067E0 to sample3.00402CE0
021EFC94  00245798  ÿW$   UNICODE "C:\$Recycle.Bin\S-1-5-21-2312279452-211
```

Fig.27 DeleteFileW



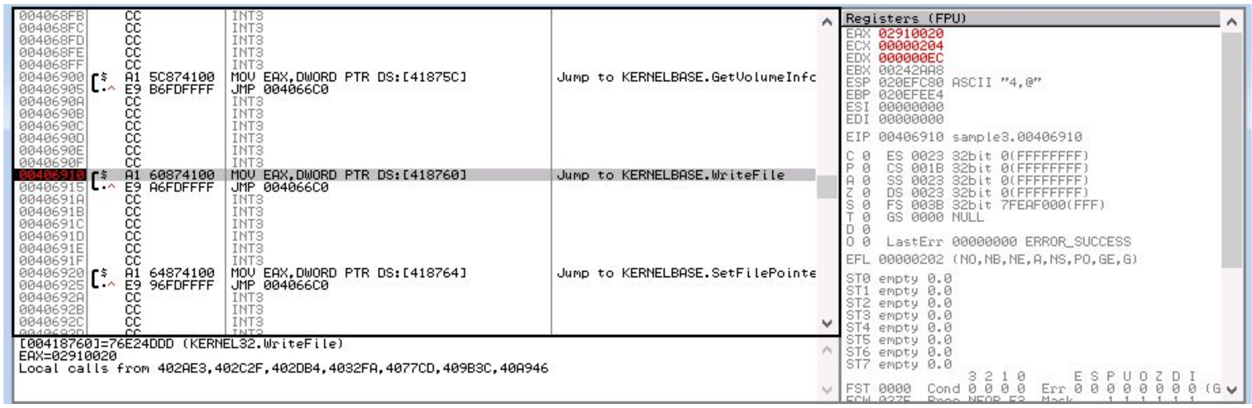
CPU - thread 20. (000009C0), module sample3

```
0040680B     CC            INT3
0040680C     CC            INT3
0040680D     CC            INT3
0040680E     CC            INT3
0040680F     CC            INT3
00406810  $  A1 14874100   MOV EAX,DWORD PTR DS:[418714]
00406815  .^ E9 A6FEFFFF   JMP 004066C0
0040681A     CC            INT3
0040681B     CC            INT3
0040681C     CC            INT3
0040681D     CC            INT3
0040681E     CC            INT3
0040681F     CC            INT3
00406820  $  A1 18874100   MOV EAX,DWORD PTR DS:[418718]            Jump to KERNELBASE.ReadFile
00406825  .^ E9 96FEFFFF   JMP 004066C0
0040682A     CC            INT3
0040682B     CC            INT3
0040682C     CC            INT3
0040682D     CC            INT3
0040682E     CC            INT3
0040682F     CC            INT3
00406830  $  A1 1C874100   MOV EAX,DWORD PTR DS:[41871C]            Jump to KERNELBASE.CreateFileW
00406835  .^ E9 86FEFFFF   JMP 004066C0
0040683A     CC            INT3
0040683B     CC            INT3
0040683C     CC            INT3
```

```
[00418718]=76E24D9B (KERNEL32.ReadFile)
EAX=0000022C (decimal 556.)
Local calls from 402A73,402E3F,4077AA
```

```
Registers (FPU)
EAX 0000022C
ECX 000FFFF0
EDX 0260A020
EBX 00242AA8
ESP 021EFC80 ASCII "x*@"
EBP 021EFEE4
ESI 00000000
EDI 00000000

EIP 00406820 sample3.00406820

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FEAE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr 00000000 ERROR_SUCCESS

EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0 (G
```

Fig.28 ReadFile

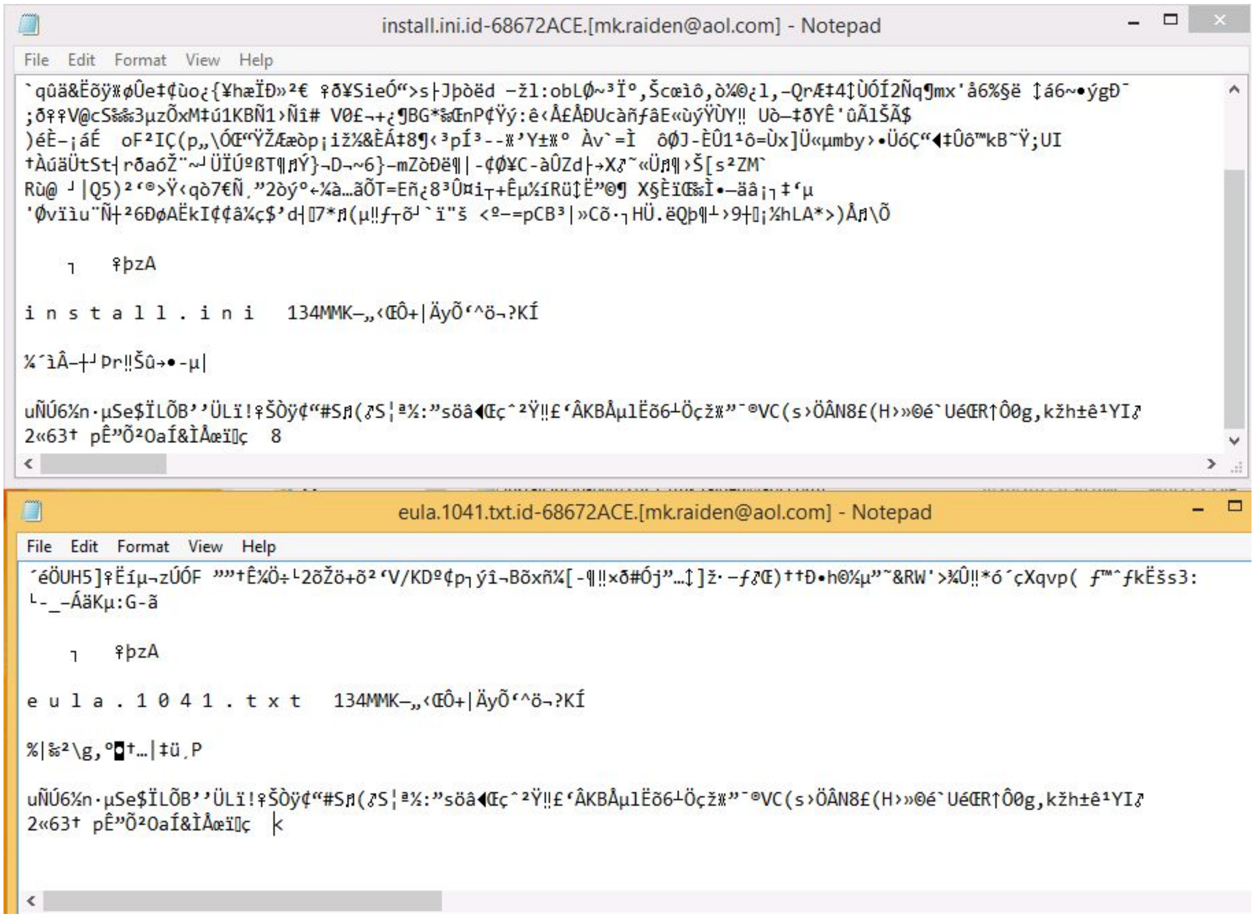


```
004068FB     CC            INT3
004068FC     CC            INT3
004068FD     CC            INT3
004068FE     CC            INT3
004068FF     CC            INT3
00406900  $  A1 5C874100   MOV EAX,DWORD PTR DS:[41875C]            Jump to KERNELBASE.GetVolumeInfc
00406905  .^ E9 B6FDFFFF   JMP 004066C0
0040690A     CC            INT3
0040690B     CC            INT3
0040690C     CC            INT3
0040690D     CC            INT3
0040690E     CC            INT3
0040690F     CC            INT3
00406910  $  A1 60874100   MOV EAX,DWORD PTR DS:[418760]            Jump to KERNELBASE.WriteFile
00406915  .^ E9 A6FDFFFF   JMP 004066C0
0040691A     CC            INT3
0040691B     CC            INT3
0040691C     CC            INT3
0040691D     CC            INT3
0040691E     CC            INT3
0040691F     CC            INT3
00406920  $  A1 64874100   MOV EAX,DWORD PTR DS:[418764]            Jump to KERNELBASE.SetFilePointe
00406925  .^ E9 96FDFFFF   JMP 004066C0
0040692A     CC            INT3
0040692B     CC            INT3
0040692C     CC            INT3
```

```
[00418760]=76E24DDD (KERNEL32.WriteFile)
EAX=02910020
Local calls from 402AE3,402C2F,402DB4,4032FA,4077CD,409B3C,40A946
```

```
Registers (FPU)
EAX 02910020
ECX 00000204
EDX 000000EC
EBX 00242AA8
ESP 020EFC80 ASCII "4,@"
EBP 020EFEE4
ESI 00000000
EDI 00000000

EIP 00406910 sample3.00406910

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FEAF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr 00000000 ERROR_SUCCESS

EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0 (G
```

Fig.29 WriteFile

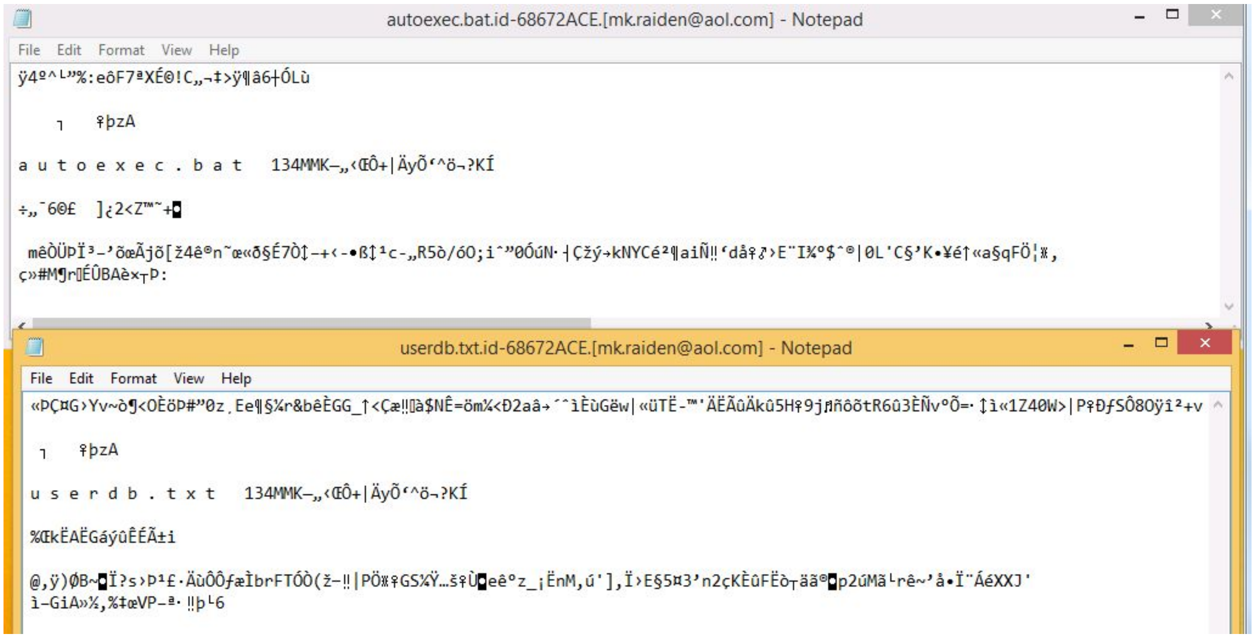

install.ini.id-68672ACE.[mk.raiden@aol.com] - Notepad
File Edit Format View Help

```
`qûä&Ëõÿ¤øÛe‡¢üo¿{¥hæÏÐ»²€ ♀ð¥SieÓ“>s├Jþòëd –ž1:obLØ~³Ï°,Šcœìô,ò%©¿1,–QrÆ‡4↨ÙÓÍ2Ñq¶mx'â6%§ë ↨á6~•ýgÐ¯
;ð♀♀V@cS‰‰3µzÕxM‡ú1KBÑ1›Ñì# V0£¬+¿¶BG*‰ŒnP¢Ÿý:ê‹Å£ÅÐUcàñƒâE«ùýŸÙY‼ Uò—‡ðYÊ'ûÃ1ŠÃ$
)éÈ–¡áÉ  oF²IÇ(p„\ÓŒ“ŸŽÆœòp¡iž¼&ÈÁ‡8¶‹³pÍ³--¤’Y±¤° Àv`=Ì  ôØJ-ÈÛ1¹ô=Ùx]Ü«µmby›•ÜóÇ“◄‡Ûô™kB˜Ÿ;UI
†ÀúäÜtSt┤rðaóŽ¨~┘ÜÏÚºßT¶♫Ý}¬D¬~6}–mZòÐë¶|-¢Ø¥C-àÛZd├→X♪˜«Ü♫¶›Š[s²ZM`
Rù@ ┘|Q5)²‘®›Ÿ‹qò7€Ñ¸”2òý°←¼à…ãÕT=Eñ¿8³Û¤i┬+Êµ½ÍRü↨Ë”©¶ X§ÈïŒ‰Ì•—äâ¡┐‡‘µ
'Øvïìu¨Ñ┼²6ÐøAËkI¢¢â¼ç$’d┤▯7*♫(µ‼ƒ┬õ┘`ï"š <º—=pCB³|»Cõ·┐HÜ.ëQþ¶┴›9┼▯¡½hLA*>)Å♫\Õ

    ┐   ♀þzA

i n s t a l l . i n i   134MMK–„‹ŒÔ+|ÄyÕ‘^ö¬?KÍ

¼´ìÂ–┼┘Þr‼Šû→•-µ|

uÑÚ6½n·µSe$ÏLÕB’’ÜLï!♀ŠÒÿ¢“#S♫(♪S¦ª½:”söâ◄Œç^²Ÿ‼£‘ÂKBÅµ1Ëõ6┴Öçž¤”¯®VC(s›ÖÂN8£(H›»©é`UéŒR↑Ô0g,kžh±ê¹YI♪
2«63† pÊ”Õ²OaÍ&ÌÅœï▯ç  8
```

eula.1041.txt.id-68672ACE.[mk.raiden@aol.com] - Notepad
File Edit Format View Help

```
´éÖUH5]♀Ëíµ¬zÚÓF ”’†Ê¼Ö÷└2õŽö+ô²‘V/KDº¢p┐ýî¬Bõxñ¾[-¶‼×ð#Ój”…↨]ž·–ƒ♪Œ)††Ð•h©½µ”˜&RW'>¾Û‼*ó´çXqvp( ƒ™^ƒkËšs3:
└-_–ÁäKµ:G-ã

    ┐   ♀þzA

e u l a . 1 0 4 1 . t x t   134MMK–„‹ŒÔ+|ÄyÕ‘^ö¬?KÍ

%|‰²\g,º▯†…|‡ü¸P

uÑÚ6½n·µSe$ÏLÕB’’ÜLï!♀ŠÒÿ¢“#S♫(♪S¦ª½:”söâ◄Œç^²Ÿ‼£‘ÂKBÅµ1Ëõ6┴Öçž¤”¯®VC(s›ÖÂN8£(H›»©é`UéŒR↑Ô0g,kžh±ê¹YI♪
2«63† pÊ”Õ²OaÍ&ÌÅœï▯ç  k
```

Fig.30 File structure from same folder

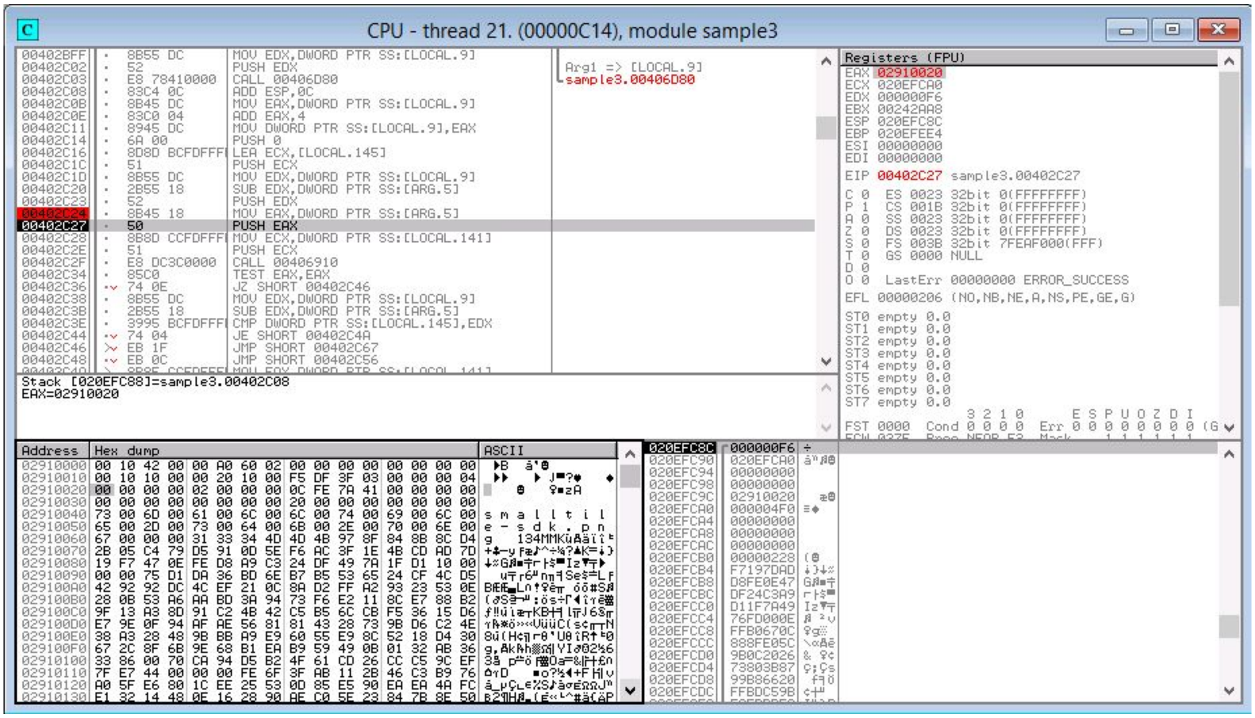

autoexec.bat.id-68672ACE.[mk.raiden@aol.com] - Notepad
File Edit Format View Help

```
ÿ4º^└”%:eôF7ªXÉ©!C„¬‡>ÿ¶â6┼ÓLù

   ┐   ♀þzA

a u t o e x e c . b a t   134MMK–„‹ŒÔ+|ÄyÕ‘^ö¬?KÍ

÷„¯6©£  ]¿2<Z™˜+▯

 mêÒÜÞÏ³–’õœÃjõ[ž4ê®n˜œ«ð§É7Ò↨-+‹-•ß↨¹c-„R5ò/6O;i^”0ÓúN·┤Çžý→kNYCé²¶aiÑ‼‘dâ♀♪›E¨I¾°$^®|0L'C§’K•¥é↑«a§qFÖ¦¤,
ç»#M¶r▯ÉÛBAèx┬Þ:
```

userdb.txt.id-68672ACE.[mk.raiden@aol.com] - Notepad
File Edit Format View Help

```
«ÞÇ¤G›Yv~ò¶<OÈöÞ#”0z¸Ee¶§¼r&bêÈGG_↑<Çæ‼▯à$NÊ=öm¼<Ð2aâ→´^ìÈùGëw|«üTË-™'ÄËÃûÄkû5H♀9j♫ñôõtR6û3ÈÑv°Õ=·↨ì«1Z40W>|P♀ÐƒSÔ8Oÿì²+v

 ┐   ♀þzA

u s e r d b . t x t   134MMK–„‹ŒÔ+|ÄyÕ‘^ö¬?KÍ

%ŒkËAËGáýûÊÉÃ±i

@,ÿ)ØB~▯Ï?s›Þ¹£·ÄùÔÔƒæÌbrFTÓÒ(ž–‼|PÖ¤♀GS¼Ÿ…š♀Ù▯eê°z_¡ËnM,ú'],Ï›E§5¤3’n2çKÈûFËò┬ãã®▯p2úMã└rê~’å•Ï¨ÁéXXJ'
ì–GiA»¼,%‡œVP–ª·‼þ└6
```

Fig.31 File structure from different folder



CPU - thread 21. (00000C14), module sample3

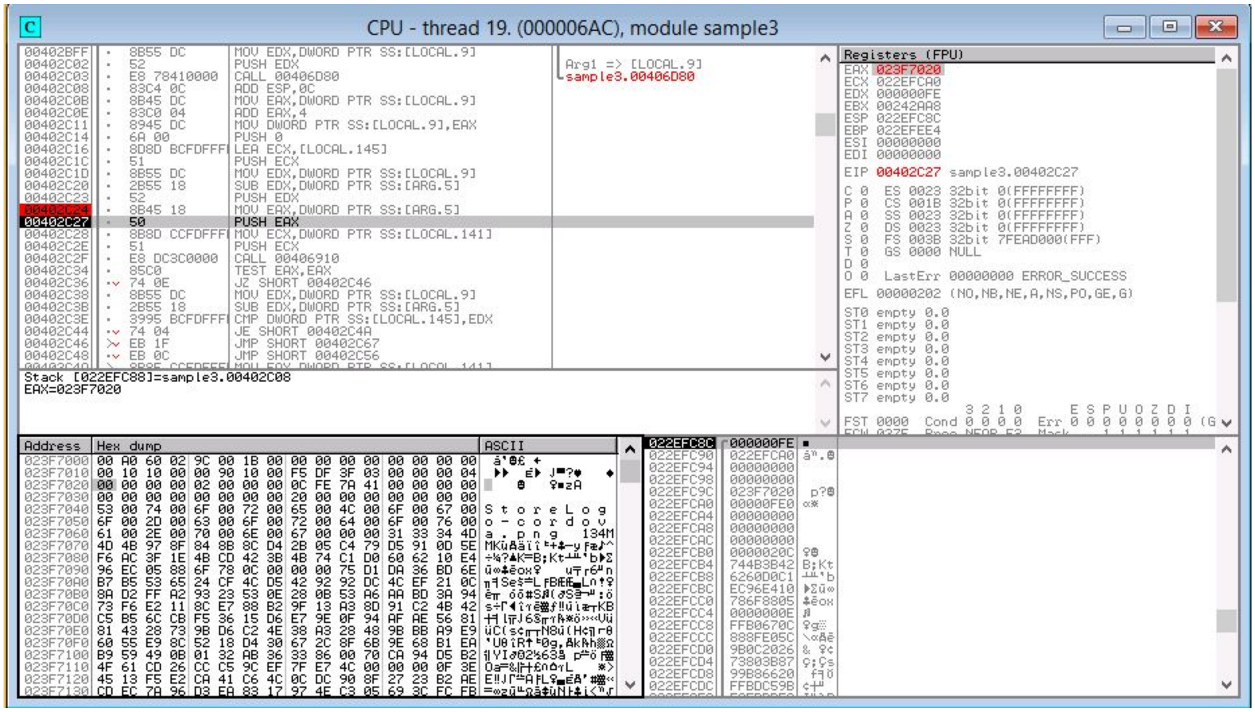
```
00402BFF  .  8B55 DC         MOV EDX,DWORD PTR SS:[LOCAL.9]      ┌Arg1 => [LOCAL.9]
00402C02  .  52              PUSH EDX                             └sample3.00406D80
00402C03  .  E8 78410000     CALL 00406D80
00402C08  .  83C4 0C         ADD ESP,0C
00402C0B  .  8B45 DC         MOV EAX,DWORD PTR SS:[LOCAL.9]
00402C0E  .  83C0 04         ADD EAX,4
00402C11  .  8945 DC         MOV DWORD PTR SS:[LOCAL.9],EAX
00402C14  .  6A 00           PUSH 0
00402C16  .  8D8D BCFDFFFF   LEA ECX,[LOCAL.145]
00402C1C  .  51              PUSH ECX
00402C1D  .  8B55 DC         MOV EDX,DWORD PTR SS:[LOCAL.9]
00402C20  .  2B55 18         SUB EDX,DWORD PTR SS:[ARG.5]
00402C23  .  52              PUSH EDX
00402C24  .  8B45 18         MOV EAX,DWORD PTR SS:[ARG.5]
00402C27  .  50              PUSH EAX
00402C28  .  8B8D CCFDFFFF   MOV ECX,DWORD PTR SS:[LOCAL.141]
00402C2E  .  51              PUSH ECX
00402C2F  .  E8 DC3C0000     CALL 00406910
00402C34  .  85C0            TEST EAX,EAX
00402C36  .v 74 0E           JZ SHORT 00402C46
00402C38  .  8B55 DC         MOV EDX,DWORD PTR SS:[LOCAL.9]
00402C3B  .  2B55 18         SUB EDX,DWORD PTR SS:[ARG.5]
00402C3E  .  3995 BCFDFFFF   CMP DWORD PTR SS:[LOCAL.145],EDX
00402C44  .v 74 04           JE SHORT 00402C4A
00402C46  >v EB 1F           JMP SHORT 00402C67
00402C48  .v EB 0C           JMP SHORT 00402C56

Stack [020EFC88]=sample3.00402C08
EAX=02910020
```

```
Registers (FPU)
EAX 02910020
ECX 020EFCA0
EDX 000000F6
EBX 00242AA8
ESP 020EFC8C
EBP 020EFEE4
ESI 00000000
EDI 00000000

EIP 00402C27 sample3.00402C27

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FEAF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr 00000000 ERROR_SUCCESS

EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0 (G
```

```
Address   Hex dump                                         ASCII
02910000  00 10 42 00 00 A0 60 02 00 00 00 00 00 00 00 00   ▶B  á'☻
02910010  00 10 10 00 00 20 10 00 F5 DF 3F 03 00 00 00 04   ▶▶   ▶ J▀?♥   ♦
02910020  00 00 00 00 02 00 00 00 0C FE 7A 41 00 00 00 00      ☻   ♀■zA
02910030  00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00
02910040  73 00 6D 00 61 00 6C 00 6C 00 74 00 69 00 6C 00  s m a l l t i l
02910050  65 00 2D 00 73 00 64 00 6B 00 2E 00 70 00 6E 00  e - s d k . p n
02910060  67 00 00 00 31 33 34 4D 4D 4B 97 8F 84 8B 8C D4  g   134MMKùÅäïî╘
02910070  2B 05 C4 79 D5 91 0D 5E F6 AC 3F 1E 4B CD AD 7D  +♣─y╒æ♪^÷¼?▲K═¡}
02910080  19 F7 47 0E FE D8 A9 C3 24 DF 49 7A 1F D1 10 00  ↓≈G♫■╪⌐├$▀Iz▼╤▶
02910090  00 00 75 D1 DA 36 BD 6E B7 B5 53 65 24 CF 4C D5    u╤┌6╜n╖╡Se$╧L╒
029100A0  42 92 92 DC 4C EF 21 0C 8A D2 FF A2 93 23 53 0E  BÆÆ▄L∩!♀è╥ óô#S♫
029100B0  28 0B 53 A6 AA BD 3A 94 73 F6 E2 11 8C E7 88 B2  (♂Sª¬╜:ös÷Γ◄îτê▓
029100C0  9F 13 A3 8D 91 C2 4B 42 C5 B5 6C CB F5 36 15 D6  ƒ‼úìæ┬KB┼╡l╦ⁿ6§╓
029100D0  E7 9E 0F 94 AF AE 56 81 81 43 28 73 9B D6 C2 4E  τ₧☼ö»«VüüC(s¢╓┬N
029100E0  38 A3 28 48 9B BB A9 E9 60 55 E9 8C 52 18 D4 30  8ú(H¢╗⌐Θ`UΘîR↑╘0
029100F0  67 2C 8F 6B 9E 68 B1 EA B9 59 49 0B 01 32 AB 36  g,Åk₧h▒Ω╣YI♂☺2½6
02910100  33 86 00 70 CA 94 D5 B2 4F 61 CD 26 CC C5 9C EF  3å p╩ö╒▓Oa═&╠┼£∩
02910110  7F E7 44 00 00 00 FE 6F 3F AB 11 2B 46 C3 B9 76  ⌂τD   ■o?½◄+F├╣v
02910120  A0 5F E6 80 1C EE 25 53 0D 85 E5 90 EA EA 4A FC  á_µÇ∟ε%S♪àσÉΩΩJⁿ
02910130  E1 32 14 48 0E 16 28 90 AE C0 5E 23 84 7B 8E 50  ß2¶H♫▬(É«└^#ä{ÄP
```

```
020EFC8C  ┌000000F6  ÷
020EFC90   020EFCA0  á‚ⁿ♫☻
020EFC94   00000000
020EFC98   00000000
020EFC9C   02910020    æ☻
020EFCA0   000004F0  ≡♦
020EFCA4   00000000
020EFCA8   00000000
020EFCAC   00000000
020EFCB0   00000228  (☻
020EFCB4   F7197DAD  ¡}↓≈
020EFCB8   D8FE0E47  G♫■╪
020EFCBC   DF24C3A9  ⌐├$▀
020EFCC0   D11F7A49  Iz▼╤
020EFCC4   76FD000E  ♫  ²v
020EFCC8   FFB0670C  ♀g░
020EFCCC   888FE05C  \αÅê
020EFCD0   9B0C2026  &  ♀¢
020EFCD4   73803B87  ç;Çs
020EFCD8   99B86620   f╕Ö
020EFCDC   FFBDC59B  ¢┼╜
```

Fig.32.1 EAX contains footer to be written to file



CPU - thread 19. (000006AC), module sample3

```
00402BFF  .  8B55 DC         MOV EDX,DWORD PTR SS:[LOCAL.9]      ┌Arg1 => [LOCAL.9]
00402C02  .  52              PUSH EDX                             └sample3.00406D80
00402C03  .  E8 78410000     CALL 00406D80
00402C08  .  83C4 0C         ADD ESP,0C
00402C0B  .  8B45 DC         MOV EAX,DWORD PTR SS:[LOCAL.9]
00402C0E  .  83C0 04         ADD EAX,4
00402C11  .  8945 DC         MOV DWORD PTR SS:[LOCAL.9],EAX
00402C14  .  6A 00           PUSH 0
00402C16  .  8D8D BCFDFFFF   LEA ECX,[LOCAL.145]
00402C1C  .  51              PUSH ECX
00402C1D  .  8B55 DC         MOV EDX,DWORD PTR SS:[LOCAL.9]
00402C20  .  2B55 18         SUB EDX,DWORD PTR SS:[ARG.5]
00402C23  .  52              PUSH EDX
00402C24  .  8B45 18         MOV EAX,DWORD PTR SS:[ARG.5]
00402C27  .  50              PUSH EAX
00402C28  .  8B8D CCFDFFFF   MOV ECX,DWORD PTR SS:[LOCAL.141]
00402C2E  .  51              PUSH ECX
00402C2F  .  E8 DC3C0000     CALL 00406910
00402C34  .  85C0            TEST EAX,EAX
00402C36  .v 74 0E           JZ SHORT 00402C46
00402C38  .  8B55 DC         MOV EDX,DWORD PTR SS:[LOCAL.9]
00402C3B  .  2B55 18         SUB EDX,DWORD PTR SS:[ARG.5]
00402C3E  .  3995 BCFDFFFF   CMP DWORD PTR SS:[LOCAL.145],EDX
00402C44  .v 74 04           JE SHORT 00402C4A
00402C46  >v EB 1F           JMP SHORT 00402C67
00402C48  .v EB 0C           JMP SHORT 00402C56

Stack [022EFC88]=sample3.00402C08
EAX=023F7020
```

```
Registers (FPU)
EAX 023F7020
ECX 022EFCA0
EDX 000000FE
EBX 00242AA8
ESP 022EFC8C
EBP 022EFEE4
ESI 00000000
EDI 00000000

EIP 00402C27 sample3.00402C27

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FEAD000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr 00000000 ERROR_SUCCESS

EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0 (G
```

```
Address   Hex dump                                         ASCII
023F7000  00 A0 60 02 9C 00 1B 00 00 00 00 00 00 00 00 00   á'☻£ ←
023F7010  00 10 10 00 00 90 10 00 F5 DF 3F 03 00 00 00 04   ▶▶  É▶ J▀?♥   ♦
023F7020  00 00 00 00 02 00 00 00 0C FE 7A 41 00 00 00 00      ☻   ♀■zA
023F7030  00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00
023F7040  53 00 74 00 6F 00 72 00 65 00 4C 00 6F 00 67 00  S t o r e L o g
023F7050  6F 00 2D 00 63 00 6F 00 72 00 64 00 6F 00 76 00  o - c o r d o v
023F7060  61 00 2E 00 70 00 6E 00 67 00 00 00 31 33 34 4D  a . p n g   134M
023F7070  4D 4B 97 8F 84 8B 8C D4 2B 05 C4 79 D5 91 0D 5E  MKùÅäïî╘+♣─y╒æ♪^
023F7080  F6 AC 3F 1E 4B CD 42 3B 4B 74 C1 D0 60 62 10 E4  ÷¼?▲K═B;Kt┴╨`b▶Σ
023F7090  96 EC 05 88 6F 78 0C 00 00 00 75 D1 DA 36 BD 6E  û∞♣êox♀   u╤┌6╜n
023F70A0  B7 B5 53 65 24 CF 4C D5 42 92 92 DC 4C EF 21 0C  ╖╡Se$╧L╒BÆÆ▄L∩!♀
023F70B0  8A D2 FF A2 93 23 53 0E 28 0B 53 A6 AA BD 3A 94  è╥ óô#S♫(♂Sª¬╜:ö
023F70C0  73 F6 E2 11 8C E7 88 B2 9F 13 A3 8D 91 C2 4B 42  s÷Γ◄îτê▓ƒ‼úìæ┬KB
023F70D0  C5 B5 6C CB F5 36 15 D6 E7 9E 0F 94 AF AE 56 81  ┼╡l╦ⁿ6§╓τ₧☼ö»«Vü
023F70E0  81 43 28 73 9B D6 C2 4E 38 A3 28 48 9B BB A9 E9  üC(s¢╓┬N8ú(H¢╗⌐Θ
023F70F0  60 55 E9 8C 52 18 D4 30 67 2C 8F 6B 9E 68 B1 EA  `UΘîR↑╘0g,Åk₧h▒Ω
023F7100  B9 59 49 0B 01 32 AB 36 33 86 00 70 CA 94 D5 B2  ╣YI♂☺2½63å p╩ö╒▓
023F7110  4F 61 CD 26 CC C5 9C EF 7F E7 4C 00 00 00 0F 3E  Oa═&╠┼£∩⌂τL   ☼>
023F7120  45 13 F5 E2 CA 41 C6 4C 0C DC 90 8F 27 23 B2 AE  E‼ⁿΓ╩A╞L♀▄ÉÅ'#▓«
023F7130  CD EC 7A 96 D3 EA 83 17 97 4E C3 05 69 3C FC FB  ═∞zû╙Ωâ↨ùN├♣i<ⁿ√
```

```
022EFC8C  ┌000000FE  ■
022EFC90   022EFCA0  áⁿ.☻
022EFC94   00000000
022EFC98   00000000
022EFC9C   023F7020   p?☻
022EFCA0   00000FE0  α☼
022EFCA4   00000000
022EFCA8   00000000
022EFCAC   00000000
022EFCB0   0000020C  ♀☻
022EFCB4   744B3B42  B;Kt
022EFCB8   6260D0C1  ┴╨`b
022EFCBC   EC96E410  ▶Σû∞
022EFCC0   786F8805  ♣êox
022EFCC4   0000000E  ♫
022EFCC8   FFB0670C  ♀g░
022EFCCC   888FE05C  \αÅê
022EFCD0   9B0C2026  &  ♀¢
022EFCD4   73803B87  ç;Çs
022EFCD8   99B86620   f╕Ö
022EFCDC   FFBDC59B  ¢┼╜
```

Fig.32.2 EAX contains footer to be written to file

Indicators Of Compromise

Though the malware exhibits no network based indicators of compromise, we can find a fair bit of host based indicators.

The malware recreates itself under the /Appdata folder as sample3.exe. This is one strong indicator that the system has potentially been compromised.

Upon execution, the malware also spawns 2 processes vssadmin.exe and conhost.exe. While conhost.exe can be seen as normal, any process that spawns vssadmin.exe can potentially be dangerous and must thus be flagged as an indicator of compromise.

Another indicator of compromise could be the autorun registry key "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\sample3.exe: "C:\Windows\System32\sample3.exe" ". This key adds the program to the list of programs that autorun on startup and can thus be seen as an indicator. The vss registry keys can also signify an indicator of compromise.

And finally the created .wallet files serve as an indicator of compromise. If the victim can observe these files not long after the malware has been executed, then he can potentially end the process and save the rest of his files.

Conclusion

Crysis is a highly advanced dangerous ransomware that is hard to mitigate once activated, hence prevention is definitely a critical priority. It uses very potent in-place encryption algorithms and is obfuscated to prevent analysis. Periodic backup of system files can help by facilitating system formats followed by system restores.