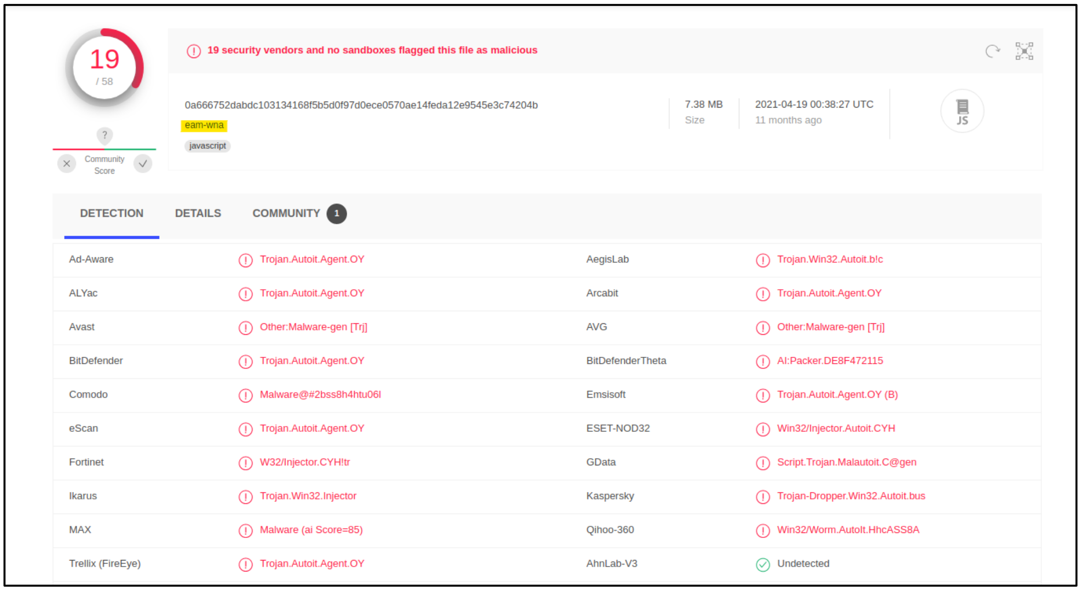
1.Virustotal

I started analyzing the malware file by uploading it to Virustotal.com to check if it is reputed or not.

Below is the screenshot of the result. From this its seen that most of the AV engines identify it by Trojan AutoIt Script.



19 security vendors and no sandboxes flagged this file as malicious

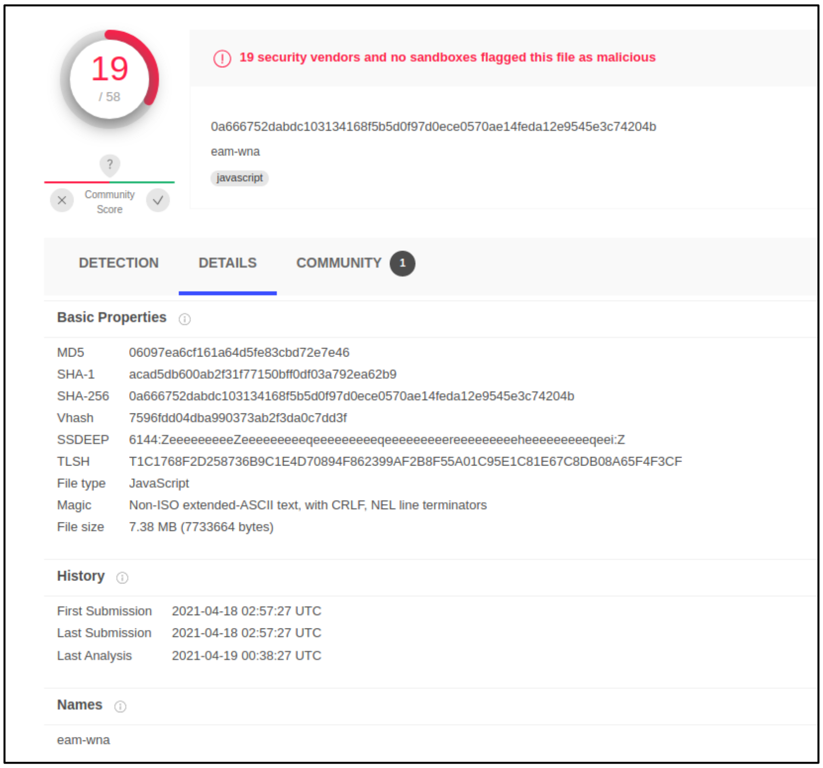
0a666752dabdc103134168f5b5d0f97d0ece0570ae14feda12e9545e3c74204b
eam-wna
javascript

7.38 MB Size

2021-04-19 00:38:27 UTC
11 months ago

Ad-Aware	Trojan.Autoit.Agent.OY	AegisLab	Trojan.Win32.Autoit.b!c
ALYac	Trojan.Autoit.Agent.OY	Arcabit	Trojan.Autoit.Agent.OY
Avast	Other:Malware-gen [Trj]	AVG	Other:Malware-gen [Trj]
BitDefender	Trojan.Autoit.Agent.OY	BitDefenderTheta	AI:Packer.DE8F472115
Comodo	Malware@#2bss8h4htu06l	Emsisoft	Trojan.Autoit.Agent.OY (B)
eScan	Trojan.Autoit.Agent.OY	ESET-NOD32	Win32/Injector.Autoit.CYH
Fortinet	W32/Injector.CYH!tr	GData	Script.Trojan.Malautoit.C@gen
Ikarus	Trojan.Win32.Injector	Kaspersky	Trojan-Dropper.Win32.Autoit.bus
MAX	Malware (ai Score=85)	Qihoo-360	Win32/Worm.AutoIt.HhcASS8A
Trellix (FireEye)	Trojan.Autoit.Agent.OY	AhnLab-V3	✓ Undetected

In the Details tab, we can see the hash values and the file type is Javascript.



19 security vendors and no sandboxes flagged this file as malicious

0a666752dabdc103134168f5b5d0f97d0ece0570ae14feda12e9545e3c74204b
eam-wna
javascript

Basic Properties

MD5	06097ea6cf161a64d5fe83cbd72e7e46
SHA-1	acad5db600ab2f31f77150bff0df03a792ea62b9
SHA-256	0a666752dabdc103134168f5b5d0f97d0ece0570ae14feda12e9545e3c74204b
Vhash	7596fdd04dba990373ab2f3da0c7dd3f
SSDEEP	6144:ZeeeeeeeeeZeeeeeeeeeqeeeeeeeeeqeeeeeeeeereeeeeeeeeheeeeeeeeeqeei:Z
TLSH	T1C1768F2D258736B9C1E4D70894F862399AF2B8F55A01C95E1C81E67C8DB08A65F4F3CF
File type	JavaScript
Magic	Non-ISO extended-ASCII text, with CRLF, NEL line terminators
File size	7.38 MB (7733664 bytes)

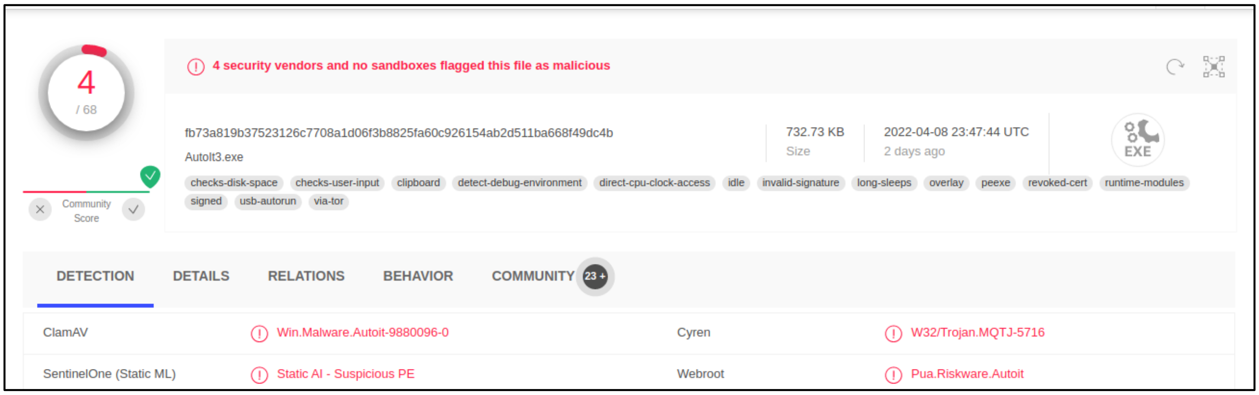
History

First Submission	2021-04-18 02:57:27 UTC
Last Submission	2021-04-18 02:57:27 UTC
Last Analysis	2021-04-19 00:38:27 UTC

Names

eam-wna

I also checked the ‘mur.exe’ application in Virustotal which was used to execute the malware file eam-wna. mur.exe was also found to be suspicious.



4 / 68

Community Score

4 security vendors and no sandboxes flagged this file as malicious

fb73a819b37523126c7708a1d06f3b8825fa60c926154ab2d511ba668f49dc4b
AutoIt3.exe

732.73 KB
Size

2022-04-08 23:47:44 UTC
2 days ago

EXE

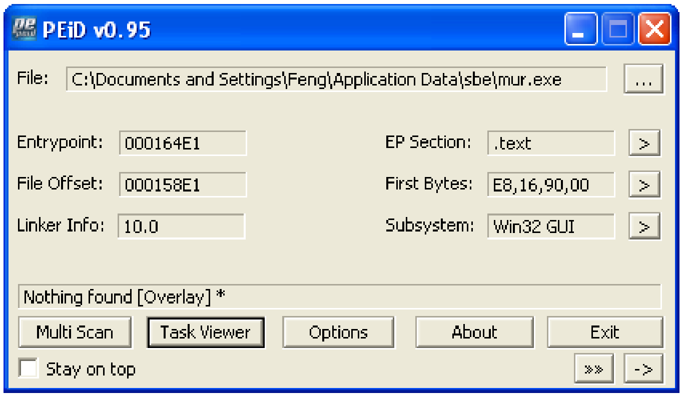
checks-disk-space checks-user-input clipboard detect-debug-environment direct-cpu-clock-access idle invalid-signature long-sleeps overlay peexe revoked-cert runtime-modules signed usb-autorun via-tor

ClamAV	Win.Malware.Autoit-9880096-0	Cyren	W32/Trojan.MQTJ-5716
SentinelOne (Static ML)	Static AI - Suspicious PE	Webroot	Pua.Riskware.Autoit

Next, I started doing the statis analysis of file mure.exe as below.

2. PeID

I used this to find if the file was packed or not and as seen it is unpacked as the EP section is .text



PEiD v0.95

File: C:\Documents and Settings\Feng\Application Data\sbe\mur.exe

Entrypoint: 000164E1

EP Section: .text

File Offset: 000158E1

First Bytes: E8,16,90,00

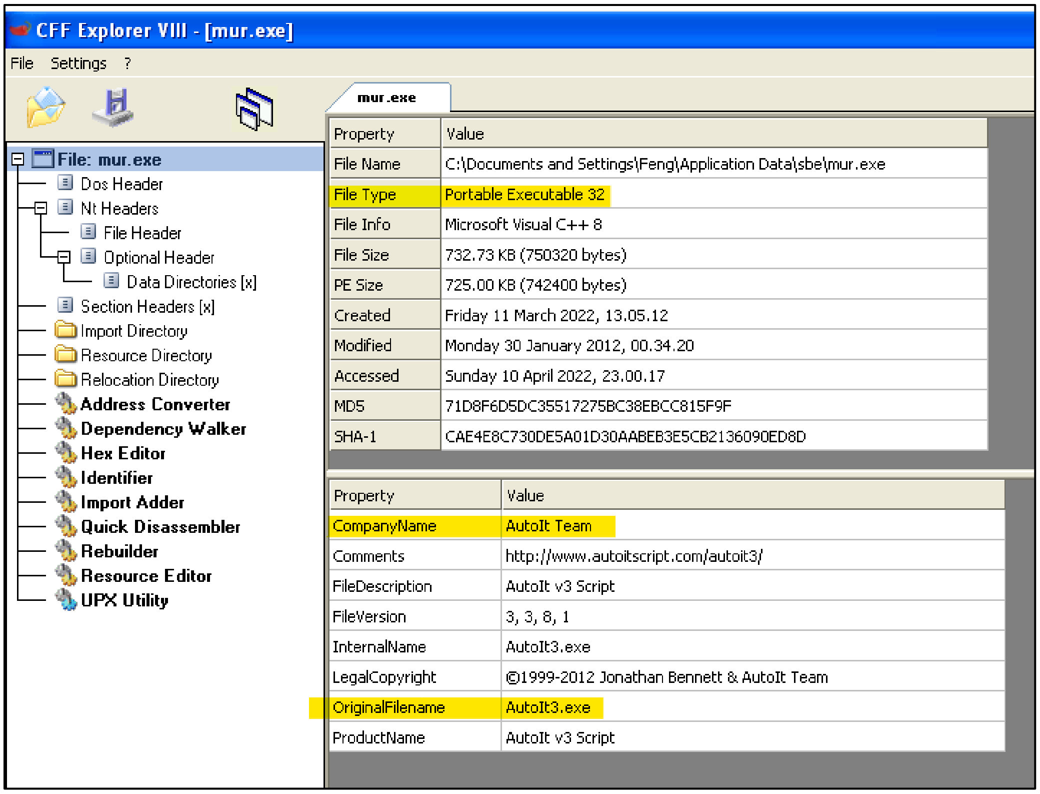
Linker Info: 10.0

Subsystem: Win32 GUI

Nothing found [Overlay] *

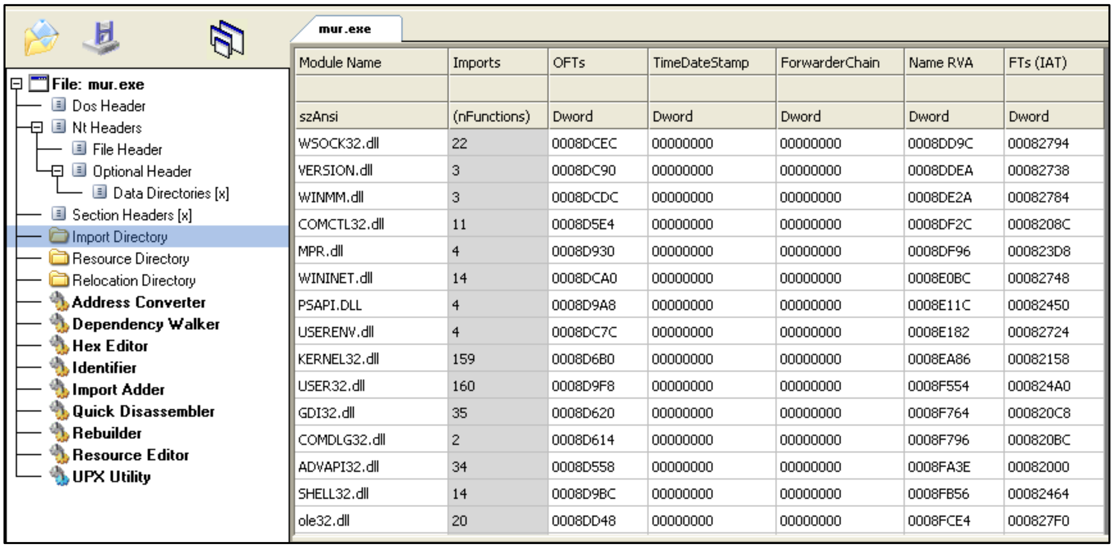
3.CFF Explorer

Used this tool to find details about the executable such as file type/ original filename, hash values and also see the imported directories as seen in below screenshot. These 16 directories in turn call various APIs.



Property	Value
File Name	C:\Documents and Settings\Feng\Application Data\sbe\mur.exe
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 8
File Size	732.73 KB (750320 bytes)
PE Size	725.00 KB (742400 bytes)
Created	Friday 11 March 2022, 13.05.12
Modified	Monday 30 January 2012, 00.34.20
Accessed	Sunday 10 April 2022, 23.00.17
MD5	71D8F6D5DC35517275BC38EBCC815F9F
SHA-1	CAE4E8C730DE5A01D30AABEB3E5CB2136090ED8D

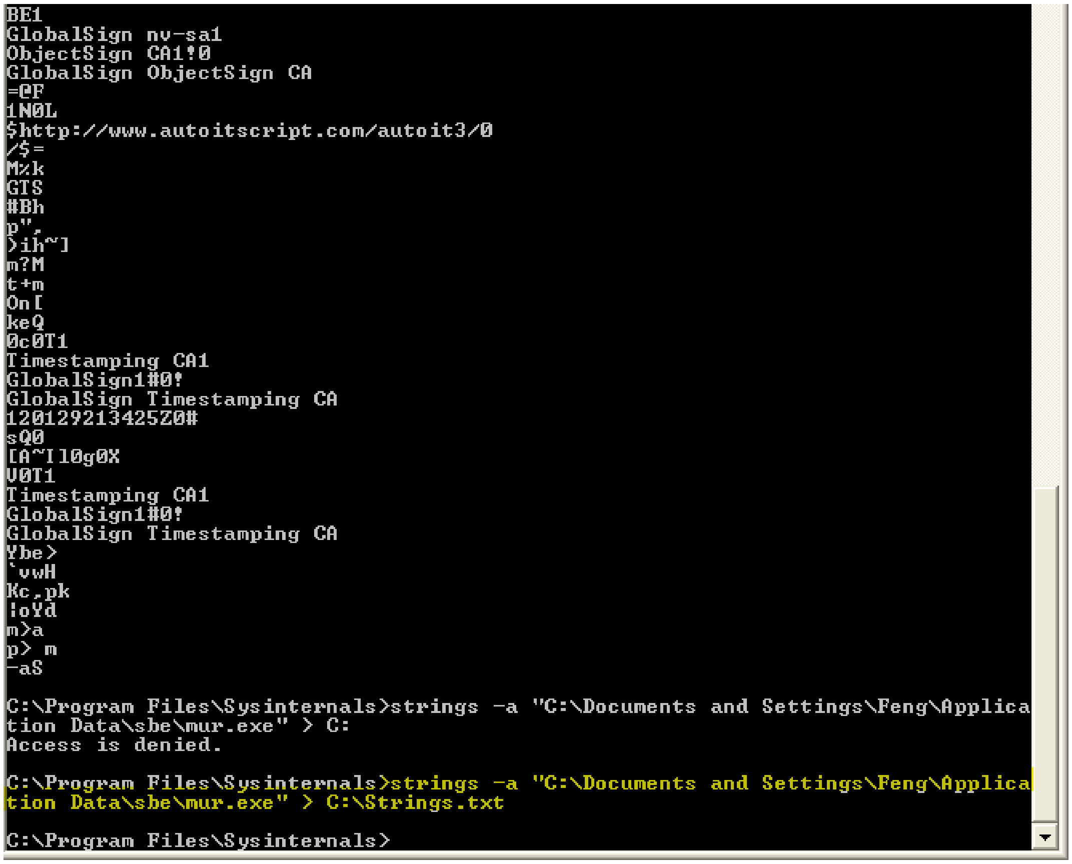
Property	Value
CompanyName	AutoIt Team
Comments	http://www.autoitscript.com/autoit3/
FileDescription	AutoIt v3 Script
FileVersion	3, 3, 8, 1
InternalName	AutoIt3.exe
LegalCopyright	©1999-2012 Jonathan Bennett & AutoIt Team
OriginalFilename	AutoIt3.exe
ProductName	AutoIt v3 Script



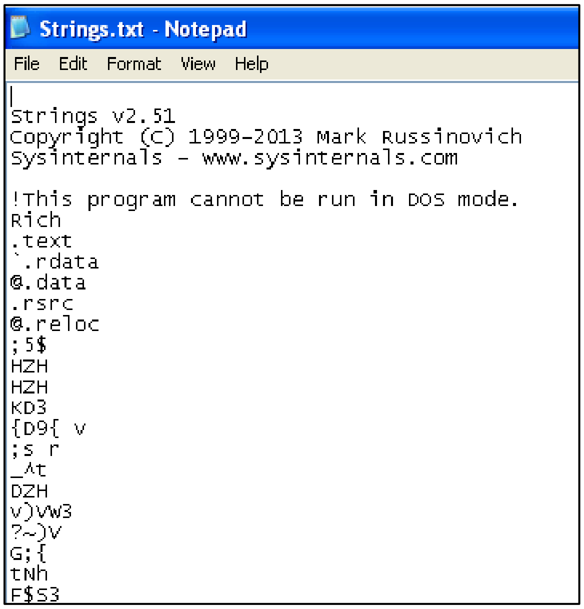
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
WSOCK32.dll	22	0008DCEC	00000000	00000000	0008DD9C	00082794
VERSION.dll	3	0008DC90	00000000	00000000	0008DDEA	00082738
WINMM.dll	3	0008DCDC	00000000	00000000	0008DE2A	00082784
COMCTL32.dll	11	0008D5E4	00000000	00000000	0008DF2C	0008208C
MPR.dll	4	0008D930	00000000	00000000	0008DF96	000823D8
WININET.dll	14	0008DCA0	00000000	00000000	0008E0BC	00082748
PSAPI.DLL	4	0008D9A8	00000000	00000000	0008E11C	00082450
USERENV.dll	4	0008DC7C	00000000	00000000	0008E182	00082724
KERNEL32.dll	159	0008D6B0	00000000	00000000	0008EA86	00082158
USER32.dll	160	0008D9F8	00000000	00000000	0008F554	000824A0
GDI32.dll	35	0008D620	00000000	00000000	0008F764	000820C8
COMDLG32.dll	2	0008D614	00000000	00000000	0008F796	000820BC
ADVAPI32.dll	34	0008D558	00000000	00000000	0008FA3E	00082000
SHELL32.dll	14	0008D9BC	00000000	00000000	0008FB56	00082464
ole32.dll	20	0008DD48	00000000	00000000	0008FCE4	000827F0

4.Strings

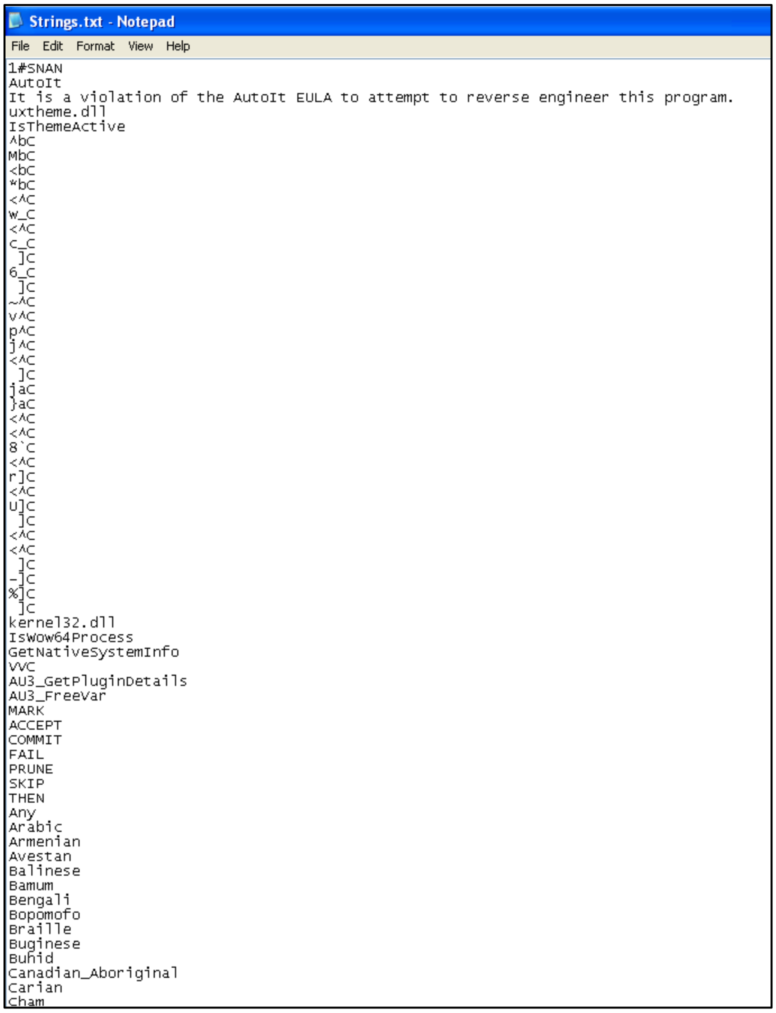
This tool was used to find for printable strings in executable file mur.exe. Below is the screenshot of the result. We can see that this exe contacted autoitscript.com and other information.



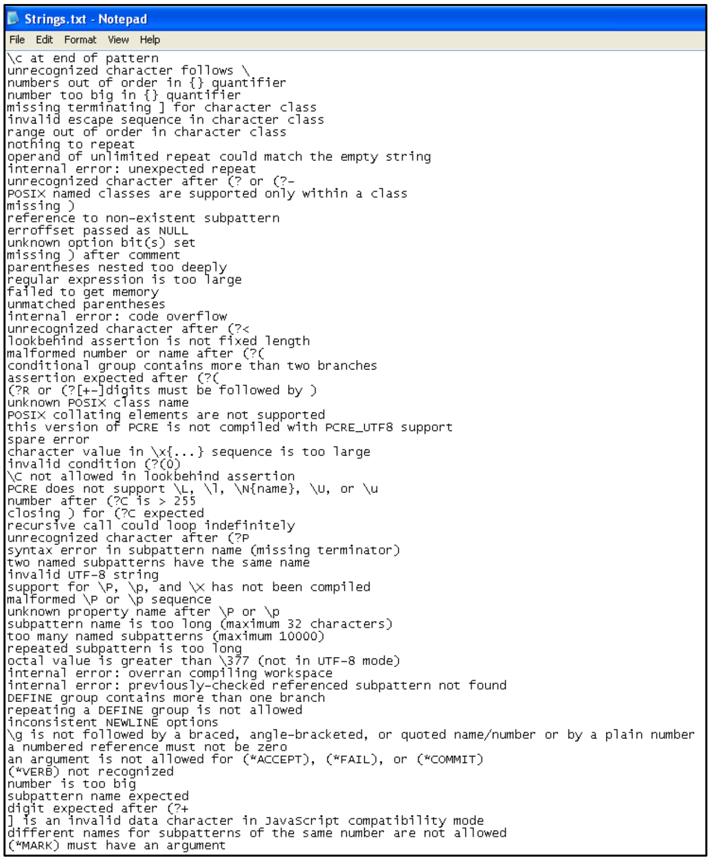
```
BE1
GlobalSign nv-sa1
ObjectSign CA1!0
GlobalSign ObjectSign CA
=@F
1N0L
$http://www.autoitscript.com/autoit3/0
/$=
M%k
GTS
#Bh
p",
)ih~]
m?M
t+m
On[
keQ
0c0T1
Timestamping CA1
GlobalSign1#0!
GlobalSign Timestamping CA
120129213425Z0#
sQ0
[A~I10g0X
V0T1
Timestamping CA1
GlobalSign1#0!
GlobalSign Timestamping CA
Ybe>
`vwH
Kc,pk
!oYd
m>a
p> m
-aS

C:\Program Files\Sysinternals>strings -a "C:\Documents and Settings\Feng\Applica
tion Data\sbe\mur.exe" > C:
Access is denied.

C:\Program Files\Sysinternals>strings -a "C:\Documents and Settings\Feng\Applica
tion Data\sbe\mur.exe" > C:\Strings.txt

C:\Program Files\Sysinternals>
```



```
Strings v2.51
Copyright (C) 1999-2013 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.rsrc
@.reloc
;5$
HZH
HZH
KD3
{D9{ v
;s r
_^t
DZH
v)Vw3
?~)V
G;{
tNh
F$S3
```



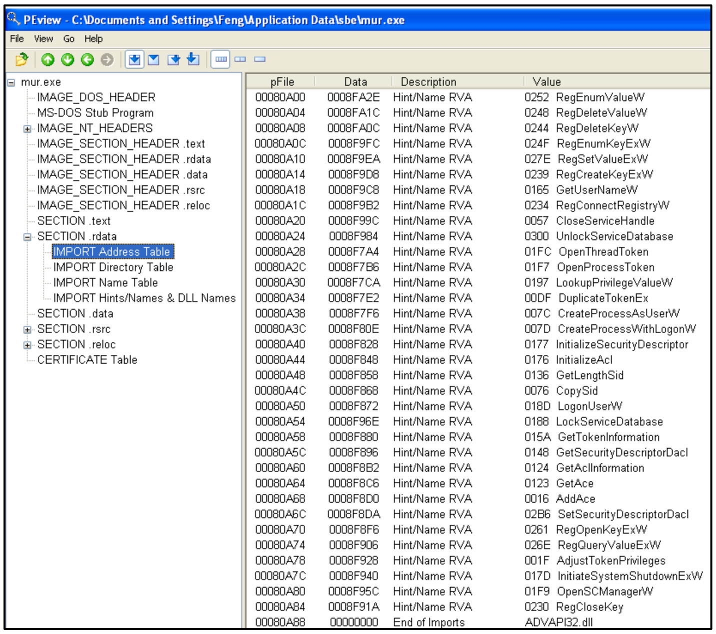
```
1#SNAN
AutoIt
It is a violation of the AutoIt EULA to attempt to reverse engineer this program.
uxtheme.dll
IsThemeActive
^bC
MbC
<bC
*bC
<^C
w_C
<^C
c_C
 ]C
6_C
 ]C
~^C
v^C
p^C
j^C
<^C
 ]C
jaC
}aC
<^C
<^C
8`C
<^C
r]C
<^C
U]C
 ]C
<^C
<^C
 ]C
-]C
%]C
 ]C
kernel32.dll
IsWow64Process
GetNativeSystemInfo
VVC
AU3_GetPluginDetails
AU3_FreeVar
MARK
ACCEPT
COMMIT
FAIL
PRUNE
SKIP
THEN
Any
Arabic
Armenian
Avestan
Balinese
Bamum
Bengali
Bopomofo
Braille
Buginese
Buhid
Canadian_Aboriginal
Carian
Cham
```



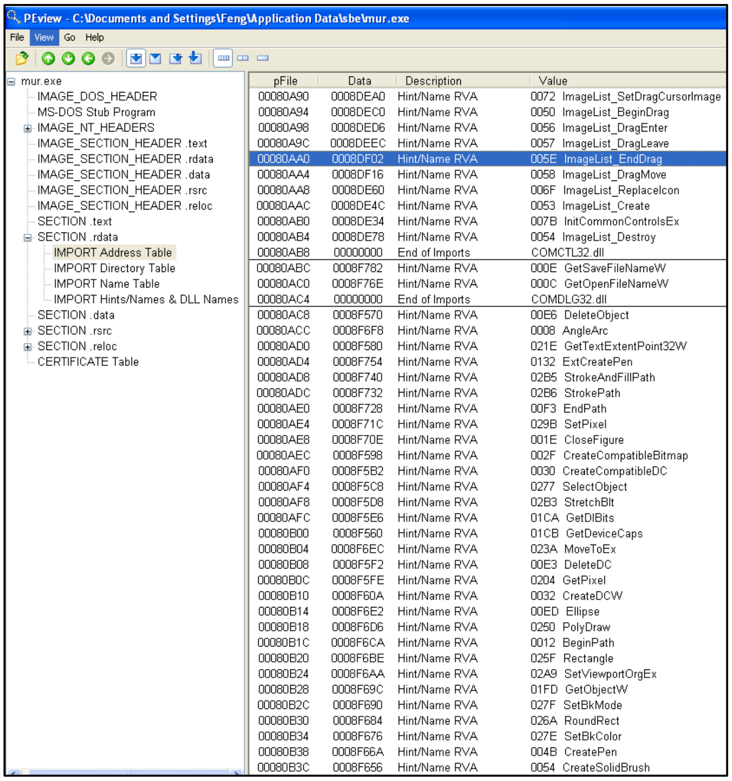
```
\c at end of pattern
unrecognized character follows \
numbers out of order in {} quantifier
number too big in {} quantifier
missing terminating ] for character class
invalid escape sequence in character class
range out of order in character class
nothing to repeat
operand of unlimited repeat could match the empty string
internal error: unexpected repeat
unrecognized character after (? or (?-
POSIX named classes are supported only within a class
missing )
reference to non-existent subpattern
erroffset passed as NULL
unknown option bit(s) set
missing ) after comment
parentheses nested too deeply
regular expression is too large
failed to get memory
unmatched parentheses
internal error: code overflow
unrecognized character after (?<
lookbehind assertion is not fixed length
malformed number or name after (?(
conditional group contains more than two branches
assertion expected after (?(
(?R or (?[+-]digits must be followed by )
unknown POSIX class name
POSIX collating elements are not supported
this version of PCRE is not compiled with PCRE_UTF8 support
spare error
character value in \x{...} sequence is too large
invalid condition (?(0)
\C not allowed in lookbehind assertion
PCRE does not support \L, \l, \N{name}, \U, or \u
number after (?C is > 255
closing ) for (?C expected
recursive call could loop indefinitely
unrecognized character after (?P
syntax error in subpattern name (missing terminator)
two named subpatterns have the same name
invalid UTF-8 string
support for \P, \p, and \X has not been compiled
malformed \P or \p sequence
unknown property name after \P or \p
subpattern name is too long (maximum 32 characters)
too many named subpatterns (maximum 10000)
repeated subpattern is too long
octal value is greater than \377 (not in UTF-8 mode)
internal error: overran compiling workspace
internal error: previously-checked referenced subpattern not found
DEFINE group contains more than one branch
repeating a DEFINE group is not allowed
inconsistent NEWLINE options
\g is not followed by a braced, angle-bracketed, or quoted name/number or by a plain number
a numbered reference must not be zero
an argument is not allowed for (*ACCEPT), (*FAIL), or (*COMMIT)
(*VERB) not recognized
number is too big
subpattern name expected
digit expected after (?+
] is an invalid data character in JavaScript compatibility mode
different names for subpatterns of the same number are not allowed
(*MARK) must have an argument
```

5. PEView

In the below screenshot, under the 'Value' column is the names of some of the imported APIs grouped by DLLs.


PEview - C:\Documents and Settings\Feng\Application Data\sbe\mur.exe
File View Go Help
mur.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .rdata
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER .rsrc
IMAGE_SECTION_HEADER .reloc
SECTION .text
SECTION .rdata
IMPORT Address Table
IMPORT Directory Table
IMPORT Name Table
IMPORT Hints/Names & DLL Names
SECTION .data
SECTION .rsrc
SECTION .reloc
CERTIFICATE Table

pFile	Data	Description	Value
00080A00	0008FA2E	Hint/Name RVA	0252 RegEnumValueW
00080A04	0008FA1C	Hint/Name RVA	0248 RegDeleteValueW
00080A08	0008FA0C	Hint/Name RVA	0244 RegDeleteKeyW
00080A0C	0008F9FC	Hint/Name RVA	024F RegEnumKeyExW
00080A10	0008F9EA	Hint/Name RVA	027E RegSetValueExW
00080A14	0008F9D8	Hint/Name RVA	0239 RegCreateKeyExW
00080A18	0008F9C8	Hint/Name RVA	0165 GetUserNameW
00080A1C	0008F9B2	Hint/Name RVA	0234 RegConnectRegistryW
00080A20	0008F99C	Hint/Name RVA	0057 CloseServiceHandle
00080A24	0008F984	Hint/Name RVA	0300 UnlockServiceDatabase
00080A28	0008F7A4	Hint/Name RVA	01FC OpenThreadToken
00080A2C	0008F7B6	Hint/Name RVA	01F7 OpenProcessToken
00080A30	0008F7CA	Hint/Name RVA	0197 LookupPrivilegeValueW
00080A34	0008F7E2	Hint/Name RVA	00DF DuplicateTokenEx
00080A38	0008F7F6	Hint/Name RVA	007C CreateProcessAsUserW
00080A3C	0008F80E	Hint/Name RVA	007D CreateProcessWithLogonW
00080A40	0008F828	Hint/Name RVA	0177 InitializeSecurityDescriptor
00080A44	0008F848	Hint/Name RVA	0176 InitializeAcl
00080A48	0008F858	Hint/Name RVA	0136 GetLengthSid
00080A4C	0008F868	Hint/Name RVA	0076 CopySid
00080A50	0008F872	Hint/Name RVA	018D LogonUserW
00080A54	0008F96E	Hint/Name RVA	0188 LockServiceDatabase
00080A58	0008F880	Hint/Name RVA	015A GetTokenInformation
00080A5C	0008F896	Hint/Name RVA	0148 GetSecurityDescriptorDacl
00080A60	0008F8B2	Hint/Name RVA	0124 GetAclInformation
00080A64	0008F8C6	Hint/Name RVA	0123 GetAce
00080A68	0008F8D0	Hint/Name RVA	0016 AddAce
00080A6C	0008F8DA	Hint/Name RVA	02B6 SetSecurityDescriptorDacl
00080A70	0008F8F6	Hint/Name RVA	0261 RegOpenKeyExW
00080A74	0008F906	Hint/Name RVA	026E RegQueryValueExW
00080A78	0008F928	Hint/Name RVA	001F AdjustTokenPrivileges
00080A7C	0008F940	Hint/Name RVA	017D InitiateSystemShutdownExW
00080A80	0008F95C	Hint/Name RVA	01F9 OpenSCManagerW
00080A84	0008F91A	Hint/Name RVA	0230 RegCloseKey
00080A88	00000000	End of Imports	ADVAPI32.dll

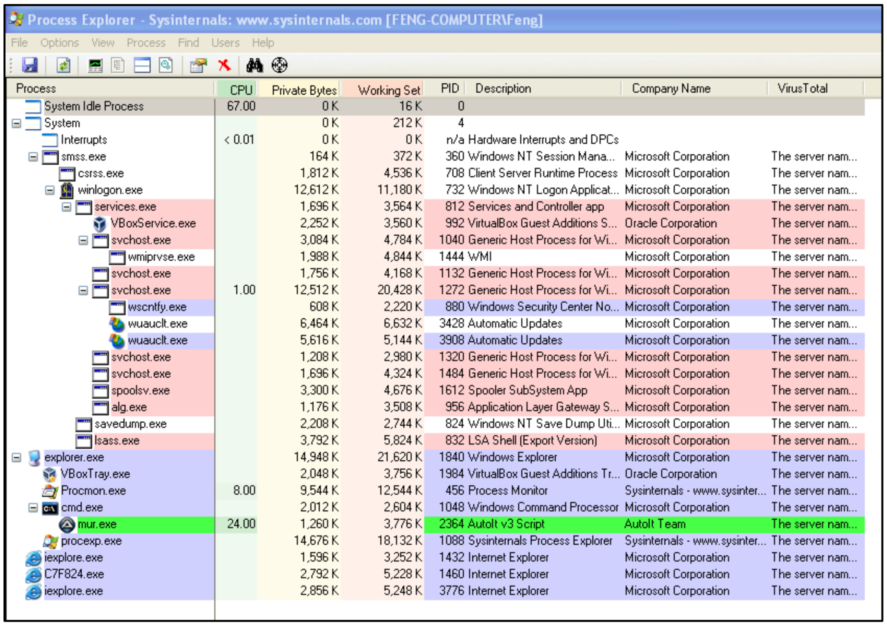

PEview - C:\Documents and Settings\Feng\Application Data\sbe\mur.exe
File
View
Go
Help

- mur.exe
  - IMAGE_DOS_HEADER
  - MS-DOS Stub Program
  - IMAGE_NT_HEADERS
  - IMAGE_SECTION_HEADER .text
  - IMAGE_SECTION_HEADER .rdata
  - IMAGE_SECTION_HEADER .data
  - IMAGE_SECTION_HEADER .rsrc
  - IMAGE_SECTION_HEADER .reloc
  - SECTION .text
  - SECTION .rdata
    - IMPORT Address Table
    - IMPORT Directory Table
    - IMPORT Name Table
    - IMPORT Hints/Names & DLL Names
  - SECTION .data
  - SECTION .rsrc
  - SECTION .reloc
  - CERTIFICATE Table

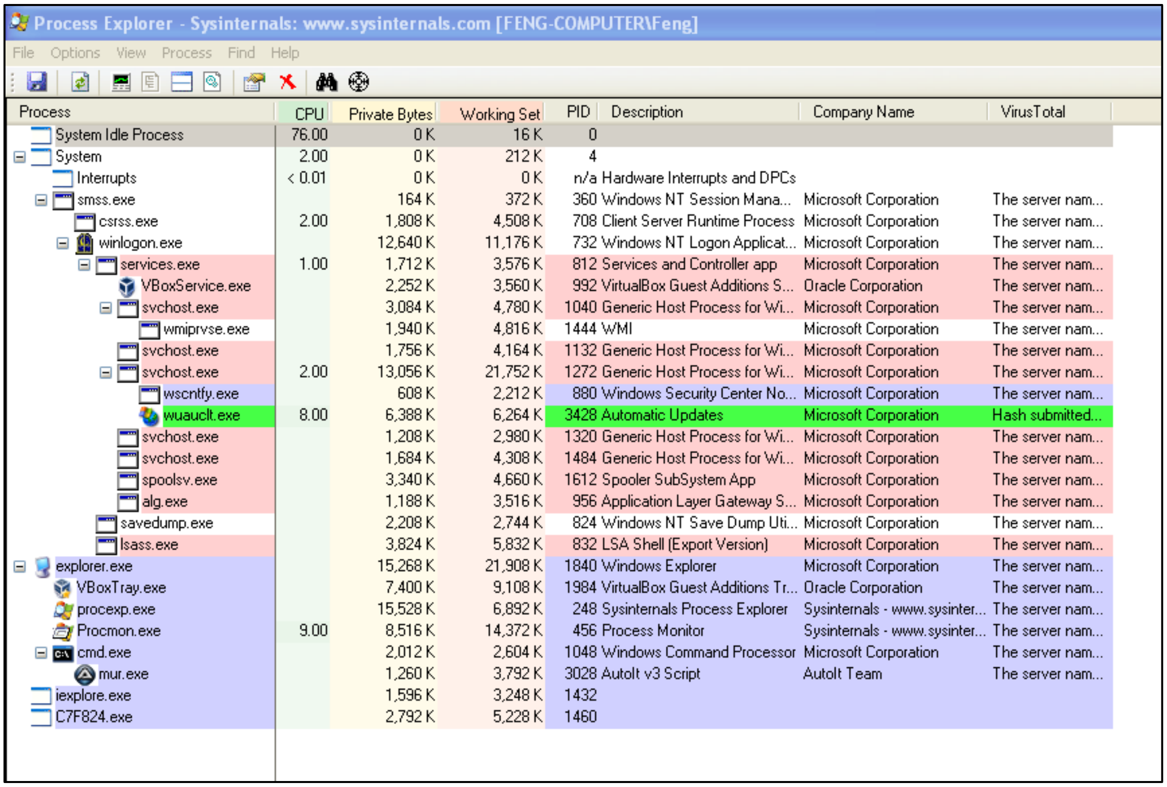
pFile	Data	Description	Value
00080A90	0008DEA0	Hint/Name RVA	0072 ImageList_SetDragCursorImage
00080A94	0008DEC0	Hint/Name RVA	0050 ImageList_BeginDrag
00080A98	0008DED6	Hint/Name RVA	0056 ImageList_DragEnter
00080A9C	0008DEEC	Hint/Name RVA	0057 ImageList_DragLeave
00080AA0	0008DF02	Hint/Name RVA	005E ImageList_EndDrag
00080AA4	0008DF16	Hint/Name RVA	0058 ImageList_DragMove
00080AA8	0008DE60	Hint/Name RVA	006F ImageList_ReplaceIcon
00080AAC	0008DE4C	Hint/Name RVA	0053 ImageList_Create
00080AB0	0008DE34	Hint/Name RVA	007B InitCommonControlsEx
00080AB4	0008DE78	Hint/Name RVA	0054 ImageList_Destroy
00080AB8	00000000	End of Imports	COMCTL32.dll
00080ABC	0008F782	Hint/Name RVA	000E GetSaveFileNameW
00080AC0	0008F76E	Hint/Name RVA	000C GetOpenFileNameW
00080AC4	00000000	End of Imports	COMDLG32.dll
00080AC8	0008F570	Hint/Name RVA	00E6 DeleteObject
00080ACC	0008F6F8	Hint/Name RVA	0008 AngleArc
00080AD0	0008F580	Hint/Name RVA	021E GetTextExtentPoint32W
00080AD4	0008F754	Hint/Name RVA	0132 ExtCreatePen
00080AD8	0008F740	Hint/Name RVA	02B5 StrokeAndFillPath
00080ADC	0008F732	Hint/Name RVA	02B6 StrokePath
00080AE0	0008F728	Hint/Name RVA	00F3 EndPath
00080AE4	0008F71C	Hint/Name RVA	029B SetPixel
00080AE8	0008F70E	Hint/Name RVA	001E CloseFigure
00080AEC	0008F598	Hint/Name RVA	002F CreateCompatibleBitmap
00080AF0	0008F5B2	Hint/Name RVA	0030 CreateCompatibleDC
00080AF4	0008F5C8	Hint/Name RVA	0277 SelectObject
00080AF8	0008F5D8	Hint/Name RVA	02B3 StretchBlt
00080AFC	0008F5E6	Hint/Name RVA	01CA GetDIBits
00080B00	0008F560	Hint/Name RVA	01CB GetDeviceCaps
00080B04	0008F6EC	Hint/Name RVA	023A MoveToEx
00080B08	0008F5F2	Hint/Name RVA	00E3 DeleteDC
00080B0C	0008F5FE	Hint/Name RVA	0204 GetPixel
00080B10	0008F60A	Hint/Name RVA	0032 CreateDCW
00080B14	0008F6E2	Hint/Name RVA	00ED Ellipse
00080B18	0008F6D6	Hint/Name RVA	0250 PolyDraw
00080B1C	0008F6CA	Hint/Name RVA	0012 BeginPath
00080B20	0008F6BE	Hint/Name RVA	025F Rectangle
00080B24	0008F6AA	Hint/Name RVA	02A9 SetViewportOrgEx
00080B28	0008F69C	Hint/Name RVA	01FD GetObjectW
00080B2C	0008F690	Hint/Name RVA	027F SetBkMode
00080B30	0008F684	Hint/Name RVA	026A RoundRect
00080B34	0008F676	Hint/Name RVA	027E SetBkColor
00080B38	0008F66A	Hint/Name RVA	004B CreatePen
00080B3C	0008F656	Hint/Name RVA	0054 CreateSolidBrush

6. Process Explorer

Using this we could find the possible processes created after running the malware from the command line. As seen in below screenshot, mur.exe starts running followed by a couple of other processes(iexplorer.exe and wuaclt.exe) getting created following it.

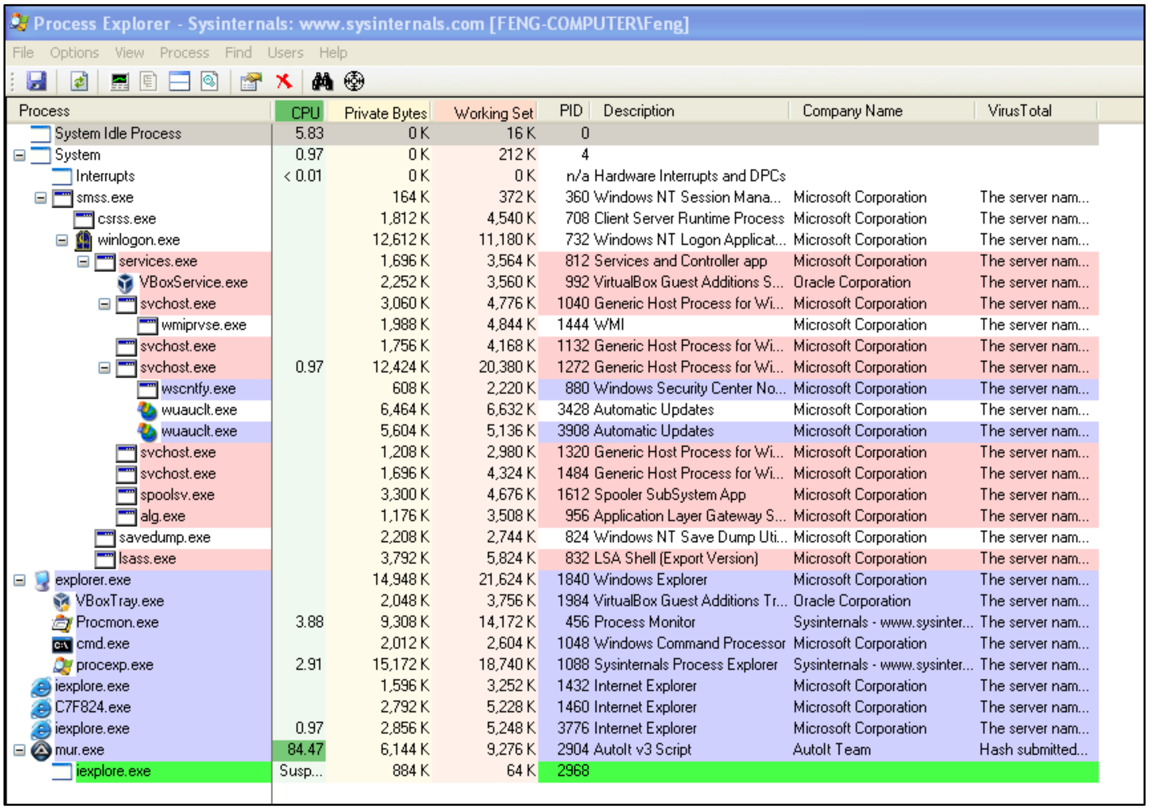

Process Explorer - Sysinternals: www.sysinternals.com [FENG-COMPUTER\Feng]
File
Options
View
Process
Find
Users
Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
System Idle Process	67.00	0 K	16 K	0			
System		0 K	212 K	4			
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs		
smss.exe		164 K	372 K	360	Windows NT Session Mana...	Microsoft Corporation	The server nam...
csrss.exe		1,812 K	4,536 K	708	Client Server Runtime Process	Microsoft Corporation	The server nam...
winlogon.exe		12,612 K	11,180 K	732	Windows NT Logon Applicat...	Microsoft Corporation	The server nam...
services.exe		1,696 K	3,564 K	812	Services and Controller app	Microsoft Corporation	The server nam...
VBoxService.exe		2,252 K	3,560 K	992	VirtualBox Guest Additions S...	Oracle Corporation	The server nam...
svchost.exe		3,084 K	4,784 K	1040	Generic Host Process for Wi...	Microsoft Corporation	The server nam...
wmiprvse.exe		1,988 K	4,844 K	1444	WMI	Microsoft Corporation	The server nam...
svchost.exe		1,756 K	4,168 K	1132	Generic Host Process for Wi...	Microsoft Corporation	The server nam...
svchost.exe	1.00	12,512 K	20,428 K	1272	Generic Host Process for Wi...	Microsoft Corporation	The server nam...
wscntfy.exe		608 K	2,220 K	880	Windows Security Center No...	Microsoft Corporation	The server nam...
wuauclt.exe		6,464 K	6,632 K	3428	Automatic Updates	Microsoft Corporation	The server nam...
wuauclt.exe		5,616 K	5,144 K	3908	Automatic Updates	Microsoft Corporation	The server nam...
svchost.exe		1,208 K	2,980 K	1320	Generic Host Process for Wi...	Microsoft Corporation	The server nam...
svchost.exe		1,696 K	4,324 K	1484	Generic Host Process for Wi...	Microsoft Corporation	The server nam...
spoolsv.exe		3,300 K	4,676 K	1612	Spooler SubSystem App	Microsoft Corporation	The server nam...
alg.exe		1,176 K	3,508 K	956	Application Layer Gateway S...	Microsoft Corporation	The server nam...
savedump.exe		2,208 K	2,744 K	824	Windows NT Save Dump Uti...	Microsoft Corporation	The server nam...
lsass.exe		3,792 K	5,824 K	832	LSA Shell (Export Version)	Microsoft Corporation	The server nam...
explorer.exe		14,948 K	21,620 K	1840	Windows Explorer	Microsoft Corporation	The server nam...
VBoxTray.exe		2,048 K	3,756 K	1984	VirtualBox Guest Additions Tr...	Oracle Corporation	The server nam...
Procmon.exe	8.00	9,544 K	12,544 K	456	Process Monitor	Sysinternals - www.sysinter...	The server nam...
cmd.exe		2,012 K	2,604 K	1048	Windows Command Processor	Microsoft Corporation	The server nam...
mur.exe	24.00	1,260 K	3,776 K	2364	AutoIt v3 Script	AutoIt Team	The server nam...
procexp.exe		14,676 K	18,132 K	1088	Sysinternals Process Explorer	Sysinternals - www.sysinter...	The server nam...
iexplore.exe		1,596 K	3,252 K	1432	Internet Explorer	Microsoft Corporation	The server nam...
C7F824.exe		2,792 K	5,228 K	1460	Internet Explorer	Microsoft Corporation	The server nam...
iexplore.exe		2,856 K	5,248 K	3776	Internet Explorer	Microsoft Corporation	The server nam...



Process Explorer - Sysinternals: www.sysinternals.com [FENG-COMPUTER\Feng]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
System Idle Process	76.00	0 K	16 K	0			
System	2.00	0 K	212 K	4			
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs		
smss.exe		164 K	372 K	360	Windows NT Session Mana...	Microsoft Corporation	The server nam...
csrss.exe	2.00	1,808 K	4,508 K	708	Client Server Runtime Process	Microsoft Corporation	The server nam...
winlogon.exe		12,640 K	11,176 K	732	Windows NT Logon Applicat...	Microsoft Corporation	The server nam...
services.exe	1.00	1,712 K	3,576 K	812	Services and Controller app	Microsoft Corporation	The server nam...
VBoxService.exe		2,252 K	3,560 K	992	VirtualBox Guest Additions S...	Oracle Corporation	The server nam...
svchost.exe		3,084 K	4,780 K	1040	Generic Host Process for Wi...	Microsoft Corporation	The server nam...
wmiprvse.exe		1,940 K	4,816 K	1444	WMI	Microsoft Corporation	The server nam...
svchost.exe		1,756 K	4,164 K	1132	Generic Host Process for Wi...	Microsoft Corporation	The server nam...
svchost.exe	2.00	13,056 K	21,752 K	1272	Generic Host Process for Wi...	Microsoft Corporation	The server nam...
wscntfy.exe		608 K	2,212 K	880	Windows Security Center No...	Microsoft Corporation	The server nam...
wuauclt.exe	8.00	6,388 K	6,264 K	3428	Automatic Updates	Microsoft Corporation	Hash submitted...
svchost.exe		1,208 K	2,980 K	1320	Generic Host Process for Wi...	Microsoft Corporation	The server nam...
svchost.exe		1,684 K	4,308 K	1484	Generic Host Process for Wi...	Microsoft Corporation	The server nam...
spoolsv.exe		3,340 K	4,660 K	1612	Spooler SubSystem App	Microsoft Corporation	The server nam...
alg.exe		1,188 K	3,516 K	956	Application Layer Gateway S...	Microsoft Corporation	The server nam...
savedump.exe		2,208 K	2,744 K	824	Windows NT Save Dump Uti...	Microsoft Corporation	The server nam...
lsass.exe		3,824 K	5,832 K	832	LSA Shell (Export Version)	Microsoft Corporation	The server nam...
explorer.exe		15,268 K	21,908 K	1840	Windows Explorer	Microsoft Corporation	The server nam...
VBoxTray.exe		7,400 K	9,108 K	1984	VirtualBox Guest Additions Tr...	Oracle Corporation	The server nam...
procexp.exe		15,528 K	6,892 K	248	Sysinternals Process Explorer	Sysinternals - www.sysinter...	The server nam...
Procmon.exe	9.00	8,516 K	14,372 K	456	Process Monitor	Sysinternals - www.sysinter...	The server nam...
cmd.exe		2,012 K	2,604 K	1048	Windows Command Processor	Microsoft Corporation	The server nam...
mur.exe		1,260 K	3,792 K	3028	AutoIt v3 Script	AutoIt Team	The server nam...
iexplore.exe		1,596 K	3,248 K	1432			
C7F824.exe		2,792 K	5,228 K	1460			

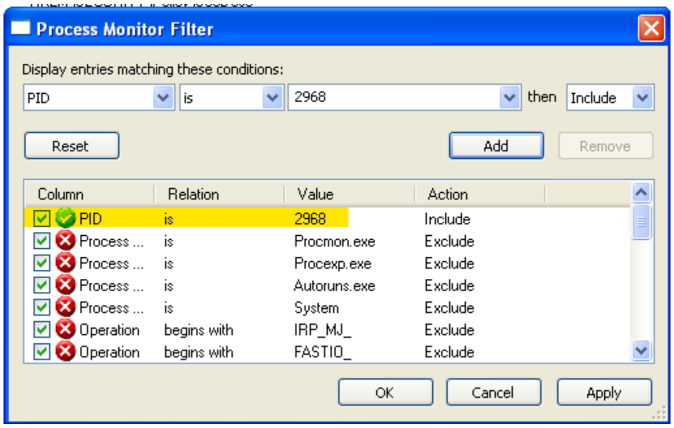


Process Explorer - Sysinternals: www.sysinternals.com [FENG-COMPUTER\Feng]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
System Idle Process	5.83	0 K	16 K	0			
System	0.97	0 K	212 K	4			
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs		
smss.exe		164 K	372 K	360	Windows NT Session Mana...	Microsoft Corporation	The server nam...
csrss.exe		1,812 K	4,540 K	708	Client Server Runtime Process	Microsoft Corporation	The server nam...
winlogon.exe		12,612 K	11,180 K	732	Windows NT Logon Applicat...	Microsoft Corporation	The server nam...
services.exe		1,696 K	3,564 K	812	Services and Controller app	Microsoft Corporation	The server nam...
VBoxService.exe		2,252 K	3,560 K	992	VirtualBox Guest Additions S...	Oracle Corporation	The server nam...
svchost.exe		3,060 K	4,776 K	1040	Generic Host Process for Wi...	Microsoft Corporation	The server nam...
wmiprvse.exe		1,988 K	4,844 K	1444	WMI	Microsoft Corporation	The server nam...
svchost.exe		1,756 K	4,168 K	1132	Generic Host Process for Wi...	Microsoft Corporation	The server nam...
svchost.exe	0.97	12,424 K	20,380 K	1272	Generic Host Process for Wi...	Microsoft Corporation	The server nam...
wscntfy.exe		608 K	2,220 K	880	Windows Security Center No...	Microsoft Corporation	The server nam...
wuauclt.exe		6,464 K	6,632 K	3428	Automatic Updates	Microsoft Corporation	The server nam...
wuauclt.exe		5,604 K	5,136 K	3908	Automatic Updates	Microsoft Corporation	The server nam...
svchost.exe		1,208 K	2,980 K	1320	Generic Host Process for Wi...	Microsoft Corporation	The server nam...
svchost.exe		1,696 K	4,324 K	1484	Generic Host Process for Wi...	Microsoft Corporation	The server nam...
spoolsv.exe		3,300 K	4,676 K	1612	Spooler SubSystem App	Microsoft Corporation	The server nam...
alg.exe		1,176 K	3,508 K	956	Application Layer Gateway S...	Microsoft Corporation	The server nam...
savedump.exe		2,208 K	2,744 K	824	Windows NT Save Dump Uti...	Microsoft Corporation	The server nam...
lsass.exe		3,792 K	5,824 K	832	LSA Shell (Export Version)	Microsoft Corporation	The server nam...
explorer.exe		14,948 K	21,624 K	1840	Windows Explorer	Microsoft Corporation	The server nam...
VBoxTray.exe		2,048 K	3,756 K	1984	VirtualBox Guest Additions Tr...	Oracle Corporation	The server nam...
Procmon.exe	3.88	9,308 K	14,172 K	456	Process Monitor	Sysinternals - www.sysinter...	The server nam...
cmd.exe		2,012 K	2,604 K	1048	Windows Command Processor	Microsoft Corporation	The server nam...
procexp.exe	2.91	15,172 K	18,740 K	1088	Sysinternals Process Explorer	Sysinternals - www.sysinter...	The server nam...
iexplore.exe		1,596 K	3,252 K	1432	Internet Explorer	Microsoft Corporation	The server nam...
C7F824.exe		2,792 K	5,228 K	1460	Internet Explorer	Microsoft Corporation	The server nam...
iexplore.exe	0.97	2,856 K	5,248 K	3776	Internet Explorer	Microsoft Corporation	The server nam...
mur.exe	84.47	6,144 K	9,276 K	2904	AutoIt v3 Script	AutoIt Team	Hash submitted...
iexplore.exe	Susp...	884 K	64 K	2968			

7. Process Monitor

From the processes getting created above, I filtered using the PID of process iexplorer.exe and observed that it was doing multiple operations such as creating files, reading registry keys and loading dlls.

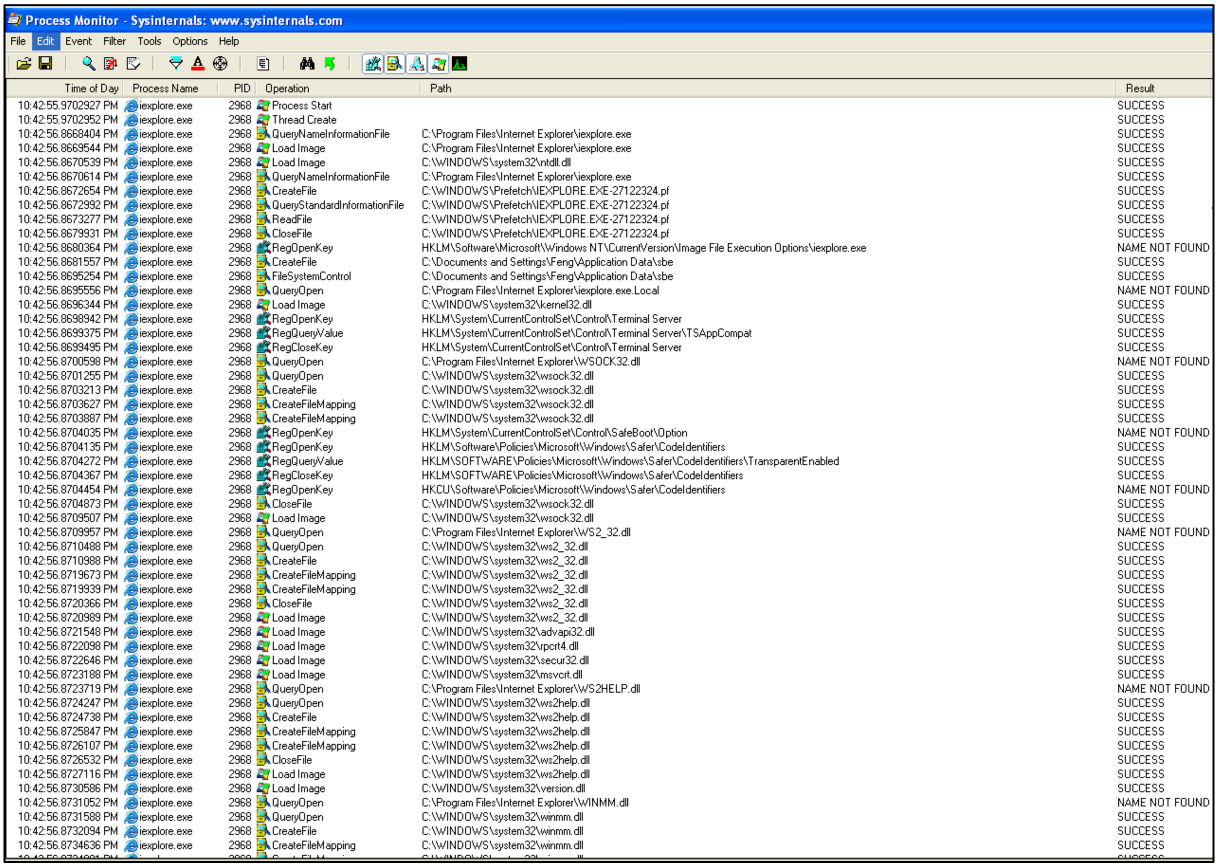


Process Monitor Filter

Display entries matching these conditions:

PID | is | 2968 | then Include

Column	Relation	Value	Action
☑ PID	is	2968	Include
☑ Process ...	is	Procmon.exe	Exclude
☑ Process ...	is	Procexp.exe	Exclude
☑ Process ...	is	Autoruns.exe	Exclude
☑ Process ...	is	System	Exclude
☑ Operation	begins with	IRP_MJ_	Exclude
☑ Operation	begins with	FASTIO_	Exclude

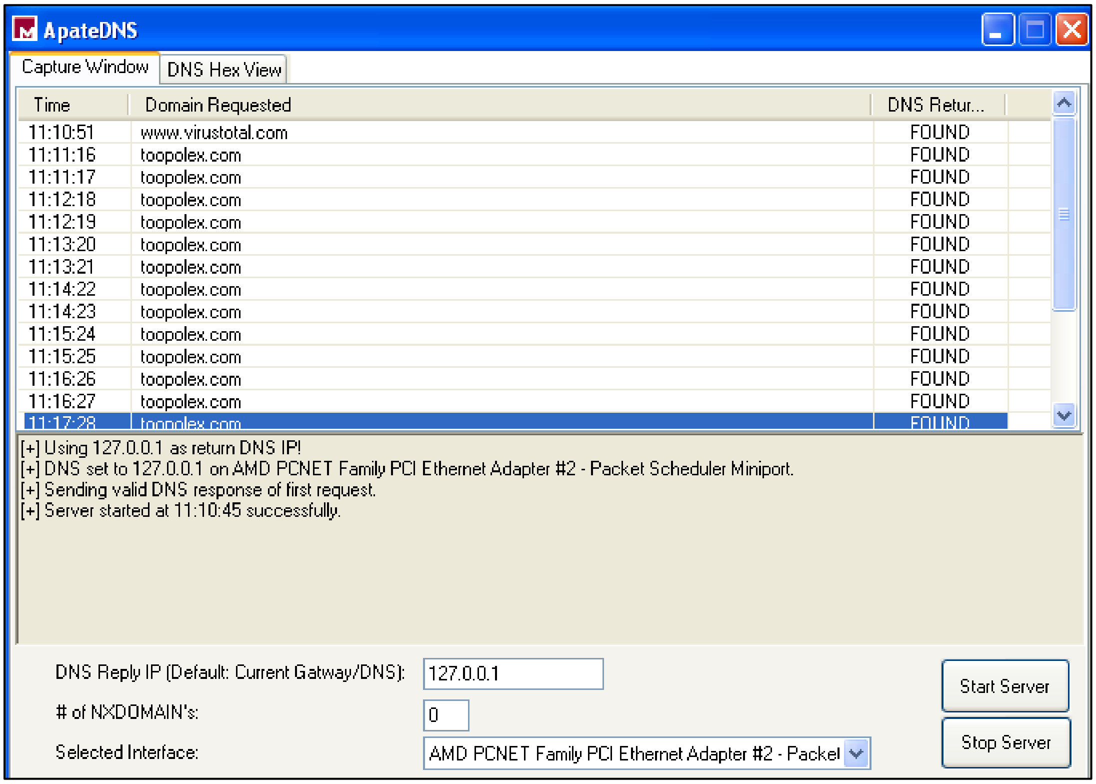


Process Monitor - Sysinternals: www.sysinternals.com

```
Time of Day          Process Name   PID   Operation                    Path                                                                                   Result
10:42:55.9702927 PM  iexplore.exe   2968  Process Start                                                                                                        SUCCESS
10:42:55.9702952 PM  iexplore.exe   2968  Thread Create                                                                                                        SUCCESS
10:42:56.8668404 PM  iexplore.exe   2968  QueryNameInformationFile     C:\Program Files\Internet Explorer\iexplore.exe                                        SUCCESS
10:42:56.8669544 PM  iexplore.exe   2968  Load Image                   C:\Program Files\Internet Explorer\iexplore.exe                                        SUCCESS
10:42:56.8670539 PM  iexplore.exe   2968  Load Image                   C:\WINDOWS\system32\ntdll.dll                                                          SUCCESS
10:42:56.8670614 PM  iexplore.exe   2968  QueryNameInformationFile     C:\Program Files\Internet Explorer\iexplore.exe                                        SUCCESS
10:42:56.8672654 PM  iexplore.exe   2968  CreateFile                   C:\WINDOWS\Prefetch\IEXPLORE.EXE-27122324.pf                                          SUCCESS
10:42:56.8672992 PM  iexplore.exe   2968  QueryStandardInformationFile C:\WINDOWS\Prefetch\IEXPLORE.EXE-27122324.pf                                          SUCCESS
10:42:56.8673277 PM  iexplore.exe   2968  ReadFile                     C:\WINDOWS\Prefetch\IEXPLORE.EXE-27122324.pf                                          SUCCESS
10:42:56.8679931 PM  iexplore.exe   2968  CloseFile                    C:\WINDOWS\Prefetch\IEXPLORE.EXE-27122324.pf                                          SUCCESS
10:42:56.8680364 PM  iexplore.exe   2968  RegOpenKey                   HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\iexplore.exe  NAME NOT FOUND
10:42:56.8681557 PM  iexplore.exe   2968  CreateFile                   C:\Documents and Settings\Feng\Application Data\sbe                                    SUCCESS
10:42:56.8695254 PM  iexplore.exe   2968  FileSystemControl            C:\Documents and Settings\Feng\Application Data\sbe                                    SUCCESS
10:42:56.8695556 PM  iexplore.exe   2968  QueryOpen                    C:\Program Files\Internet Explorer\iexplore.exe.Local                                  NAME NOT FOUND
10:42:56.8696344 PM  iexplore.exe   2968  Load Image                   C:\WINDOWS\system32\kernel32.dll                                                       SUCCESS
10:42:56.8698942 PM  iexplore.exe   2968  RegOpenKey                   HKLM\System\CurrentControlSet\Control\Terminal Server                                  SUCCESS
10:42:56.8699375 PM  iexplore.exe   2968  RegQueryValue                HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat                      SUCCESS
10:42:56.8699495 PM  iexplore.exe   2968  RegCloseKey                  HKLM\System\CurrentControlSet\Control\Terminal Server                                  SUCCESS
10:42:56.8700598 PM  iexplore.exe   2968  QueryOpen                    C:\Program Files\Internet Explorer\WSOCK32.dll                                         NAME NOT FOUND
10:42:56.8701255 PM  iexplore.exe   2968  QueryOpen                    C:\WINDOWS\system32\wsock32.dll                                                        SUCCESS
10:42:56.8703213 PM  iexplore.exe   2968  CreateFile                   C:\WINDOWS\system32\wsock32.dll                                                        SUCCESS
10:42:56.8703627 PM  iexplore.exe   2968  CreateFileMapping            C:\WINDOWS\system32\wsock32.dll                                                        SUCCESS
10:42:56.8703887 PM  iexplore.exe   2968  CreateFileMapping            C:\WINDOWS\system32\wsock32.dll                                                        SUCCESS
10:42:56.8704035 PM  iexplore.exe   2968  RegOpenKey                   HKLM\System\CurrentControlSet\Control\SafeBoot\Option                                  NAME NOT FOUND
10:42:56.8704135 PM  iexplore.exe   2968  RegOpenKey                   HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers                         SUCCESS
10:42:56.8704272 PM  iexplore.exe   2968  RegQueryValue                HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled      SUCCESS
10:42:56.8704367 PM  iexplore.exe   2968  RegCloseKey                  HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers                         SUCCESS
10:42:56.8704454 PM  iexplore.exe   2968  RegOpenKey                   HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers                         NAME NOT FOUND
10:42:56.8704873 PM  iexplore.exe   2968  CloseFile                    C:\WINDOWS\system32\wsock32.dll                                                        SUCCESS
10:42:56.8709507 PM  iexplore.exe   2968  Load Image                   C:\WINDOWS\system32\wsock32.dll                                                        SUCCESS
10:42:56.8709957 PM  iexplore.exe   2968  QueryOpen                    C:\Program Files\Internet Explorer\WS2_32.dll                                          NAME NOT FOUND
10:42:56.8710488 PM  iexplore.exe   2968  QueryOpen                    C:\WINDOWS\system32\ws2_32.dll                                                         SUCCESS
10:42:56.8710988 PM  iexplore.exe   2968  CreateFile                   C:\WINDOWS\system32\ws2_32.dll                                                         SUCCESS
10:42:56.8719673 PM  iexplore.exe   2968  CreateFileMapping            C:\WINDOWS\system32\ws2_32.dll                                                         SUCCESS
10:42:56.8719939 PM  iexplore.exe   2968  CreateFileMapping            C:\WINDOWS\system32\ws2_32.dll                                                         SUCCESS
10:42:56.8720366 PM  iexplore.exe   2968  CloseFile                    C:\WINDOWS\system32\ws2_32.dll                                                         SUCCESS
10:42:56.8720989 PM  iexplore.exe   2968  Load Image                   C:\WINDOWS\system32\ws2_32.dll                                                         SUCCESS
10:42:56.8721548 PM  iexplore.exe   2968  Load Image                   C:\WINDOWS\system32\advapi32.dll                                                       SUCCESS
10:42:56.8722098 PM  iexplore.exe   2968  Load Image                   C:\WINDOWS\system32\rpcrt4.dll                                                         SUCCESS
10:42:56.8722646 PM  iexplore.exe   2968  Load Image                   C:\WINDOWS\system32\secur32.dll                                                        SUCCESS
10:42:56.8723188 PM  iexplore.exe   2968  Load Image                   C:\WINDOWS\system32\msvcrt.dll                                                         SUCCESS
10:42:56.8723719 PM  iexplore.exe   2968  QueryOpen                    C:\Program Files\Internet Explorer\WS2HELP.dll                                         NAME NOT FOUND
10:42:56.8724247 PM  iexplore.exe   2968  QueryOpen                    C:\WINDOWS\system32\ws2help.dll                                                        SUCCESS
10:42:56.8724738 PM  iexplore.exe   2968  CreateFile                   C:\WINDOWS\system32\ws2help.dll                                                        SUCCESS
10:42:56.8725847 PM  iexplore.exe   2968  CreateFileMapping            C:\WINDOWS\system32\ws2help.dll                                                        SUCCESS
10:42:56.8726107 PM  iexplore.exe   2968  CreateFileMapping            C:\WINDOWS\system32\ws2help.dll                                                        SUCCESS
10:42:56.8726532 PM  iexplore.exe   2968  CloseFile                    C:\WINDOWS\system32\ws2help.dll                                                        SUCCESS
10:42:56.8727116 PM  iexplore.exe   2968  Load Image                   C:\WINDOWS\system32\ws2help.dll                                                        SUCCESS
10:42:56.8730586 PM  iexplore.exe   2968  Load Image                   C:\WINDOWS\system32\version.dll                                                        SUCCESS
10:42:56.8731052 PM  iexplore.exe   2968  QueryOpen                    C:\Program Files\Internet Explorer\WINMM.dll                                           NAME NOT FOUND
10:42:56.8731588 PM  iexplore.exe   2968  QueryOpen                    C:\WINDOWS\system32\winmm.dll                                                          SUCCESS
10:42:56.8732094 PM  iexplore.exe   2968  CreateFile                   C:\WINDOWS\system32\winmm.dll                                                          SUCCESS
10:42:56.8734636 PM  iexplore.exe   2968  CreateFileMapping            C:\WINDOWS\system32\winmm.dll                                                          SUCCESS
```

8. ApateDNS

To check if there are any network connections made by this malware, I used ApateDNS and found that it contacted domain toopolex.com multiple times.



Time	Domain Requested	DNS Retur...
11:10:51	www.virustotal.com	FOUND
11:11:16	toopolex.com	FOUND
11:11:17	toopolex.com	FOUND
11:12:18	toopolex.com	FOUND
11:12:19	toopolex.com	FOUND
11:13:20	toopolex.com	FOUND
11:13:21	toopolex.com	FOUND
11:14:22	toopolex.com	FOUND
11:14:23	toopolex.com	FOUND
11:15:24	toopolex.com	FOUND
11:15:25	toopolex.com	FOUND
11:16:26	toopolex.com	FOUND
11:16:27	toopolex.com	FOUND
11:17:28	toopolex.com	FOUND

```
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on AMD PCNET Family PCI Ethernet Adapter #2 - Packet Scheduler Miniport.
[+] Sending valid DNS response of first request.
[+] Server started at 11:10:45 successfully.
```

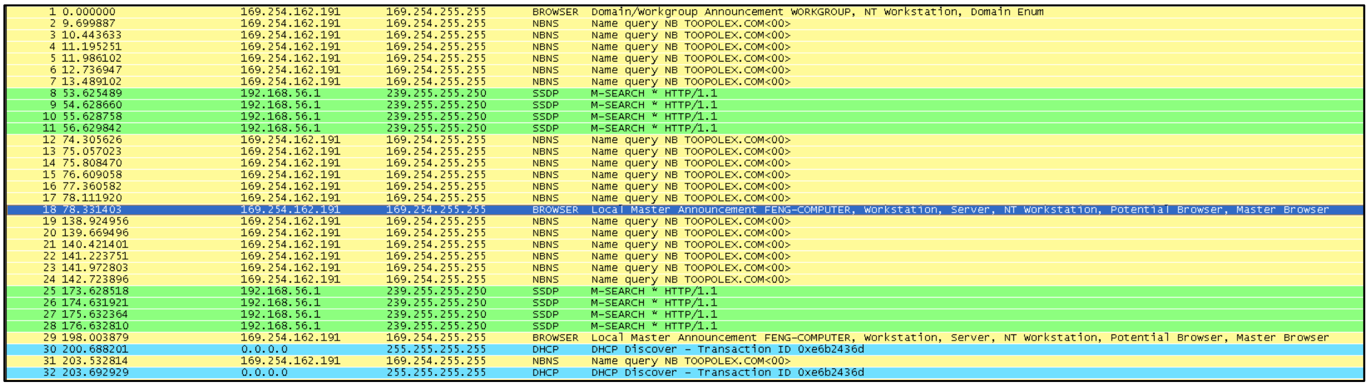
DNS Reply IP (Default: Current Gatway/DNS): 127.0.0.1

# of NXDOMAIN's: 0

Selected Interface: AMD PCNET Family PCI Ethernet Adapter #2 - Packet

9. Wireshark

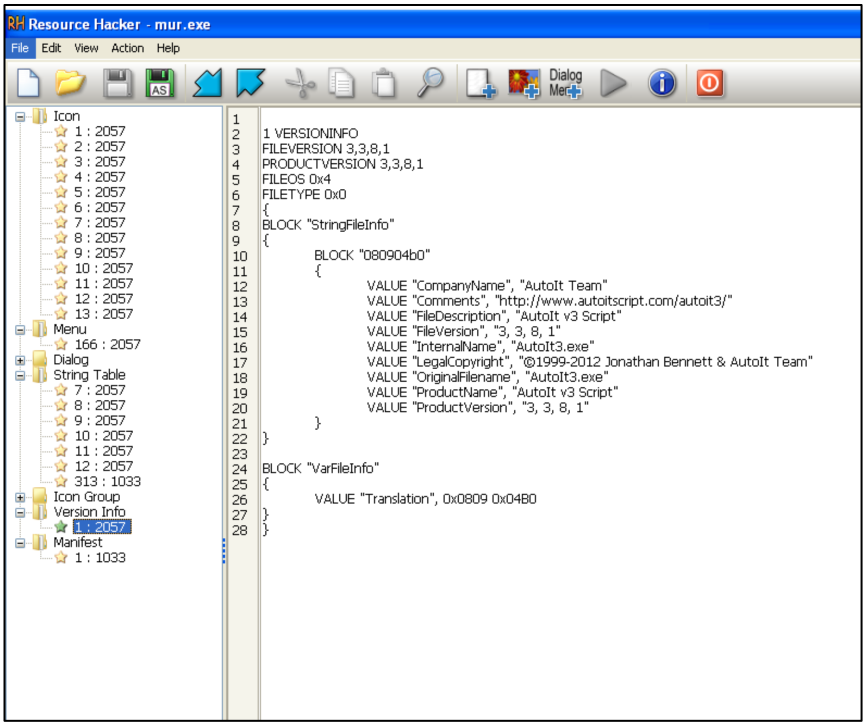
After this, I used Wireshark to capture network packets and find the IP address of the domain toopolex.com. The IP address found was 169.254.255.255.



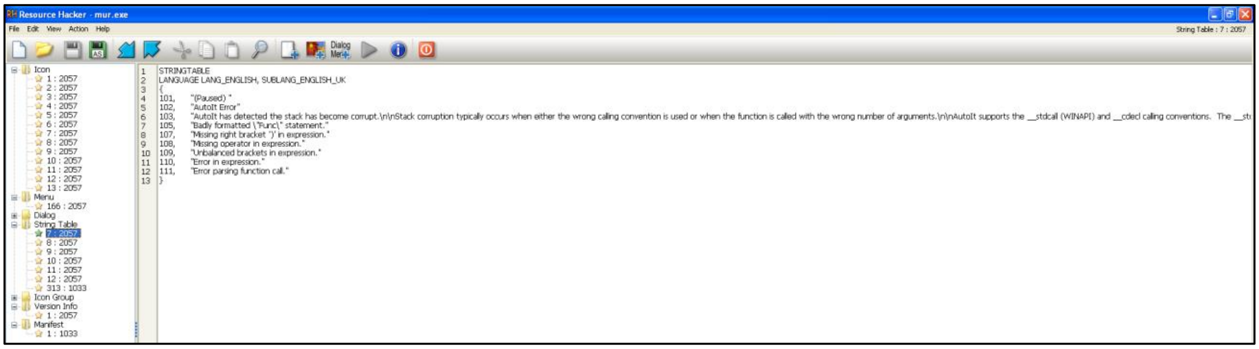
```
  1 0.000000      169.254.162.191   169.254.255.255   BROWSER  Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
  2 9.699887      169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
  3 10.443633     169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
  4 11.195251     169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
  5 11.986102     169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
  6 12.736947     169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
  7 13.489102     169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
  8 53.625489     192.168.56.1      239.255.255.250   SSDP     M-SEARCH * HTTP/1.1
  9 54.628660     192.168.56.1      239.255.255.250   SSDP     M-SEARCH * HTTP/1.1
 10 55.628758     192.168.56.1      239.255.255.250   SSDP     M-SEARCH * HTTP/1.1
 11 56.629842     192.168.56.1      239.255.255.250   SSDP     M-SEARCH * HTTP/1.1
 12 74.305626     169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
 13 75.057023     169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
 14 75.808470     169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
 15 76.609058     169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
 16 77.360582     169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
 17 78.111920     169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
 18 78.331403     169.254.162.191   169.254.255.255   BROWSER  Local Master Announcement FENG-COMPUTER, Workstation, Server, NT Workstation, Potential Browser, Master Browser
 19 138.924956    169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
 20 139.669496    169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
 21 140.421401    169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
 22 141.223751    169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
 23 141.972803    169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
 24 142.723896    169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
 25 173.628518    192.168.56.1      239.255.255.250   SSDP     M-SEARCH * HTTP/1.1
 26 174.631921    192.168.56.1      239.255.255.250   SSDP     M-SEARCH * HTTP/1.1
 27 175.632364    192.168.56.1      239.255.255.250   SSDP     M-SEARCH * HTTP/1.1
 28 176.632810    192.168.56.1      239.255.255.250   SSDP     M-SEARCH * HTTP/1.1
 29 198.003879    169.254.162.191   169.254.255.255   BROWSER  Local Master Announcement FENG-COMPUTER, Workstation, Server, NT Workstation, Potential Browser, Master Browser
 30 200.688201    0.0.0.0           255.255.255.255   DHCP     DHCP Discover - Transaction ID 0xe6b2436d
 31 203.532814    169.254.162.191   169.254.255.255   NBNS     Name query NB TOOPOLEX.COM<00>
 32 203.692929    0.0.0.0           255.255.255.255   DHCP     DHCP Discover - Transaction ID 0xe6b2436d
```

10.Resource Hacker

Tool used to compile and decompile. Below is the information I found.



```

1 VERSIONINFO
FILEVERSION 3,3,8,1
PRODUCTVERSION 3,3,8,1
FILEOS 0x4
FILETYPE 0x0
{
BLOCK "StringFileInfo"
{
	BLOCK "080904b0"
	{
		VALUE "CompanyName", "AutoIt Team"
		VALUE "Comments", "http://www.autoitscript.com/autoit3/"
		VALUE "FileDescription", "AutoIt v3 Script"
		VALUE "FileVersion", "3, 3, 8, 1"
		VALUE "InternalName", "AutoIt3.exe"
		VALUE "LegalCopyright", "©1999-2012 Jonathan Bennett & AutoIt Team"
		VALUE "OriginalFilename", "AutoIt3.exe"
		VALUE "ProductName", "AutoIt v3 Script"
		VALUE "ProductVersion", "3, 3, 8, 1"
	}
}

BLOCK "VarFileInfo"
{
	VALUE "Translation", 0x0809 0x04B0
}
}
```



```
STRINGTABLE
LANGUAGE LANG_ENGLISH, SUBLANG_ENGLISH_UK
{
101,	"(Paused) "
102,	"AutoIt Error"
103,	"AutoIt has detected the stack has become corrupt.\n\nStack corruption typically occurs when either the wrong calling convention is used or when the function is called with the wrong number of arguments.\n\nAutoIt supports the __stdcall (WINAPI) and __cdecl calling conventions.  The __st
105,	"Badly formatted \"Func\" statement."
107,	"Missing right bracket ')' in expression."
108,	"Missing operator in expression."
109,	"Unbalanced brackets in expression."
110,	"Error in expression."
111,	"Error parsing function call."
}
```