MALWARE ANALYSIS TERM PROJECT

Initial malware execution command line: **mur.exe eam-wna**

1. Multi-stage (multiple processes) activity:

To begin with, top-down approach was followed to analyze the given malware. The malware was run from the command line and using Process Explorer, the PIDs of the processes it created were captured. Multi-stage process activity was observed as below-

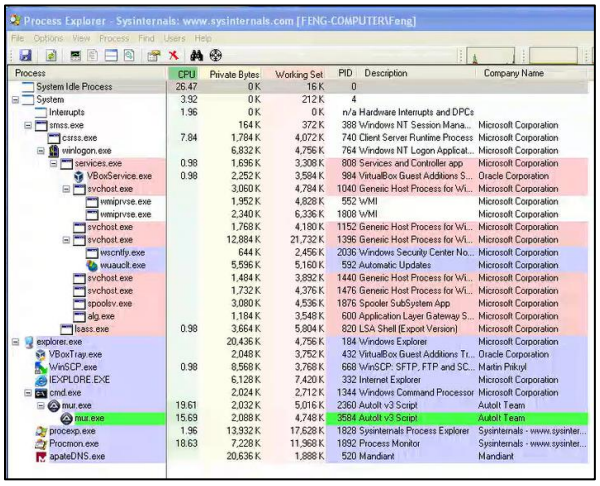
Mur.exe

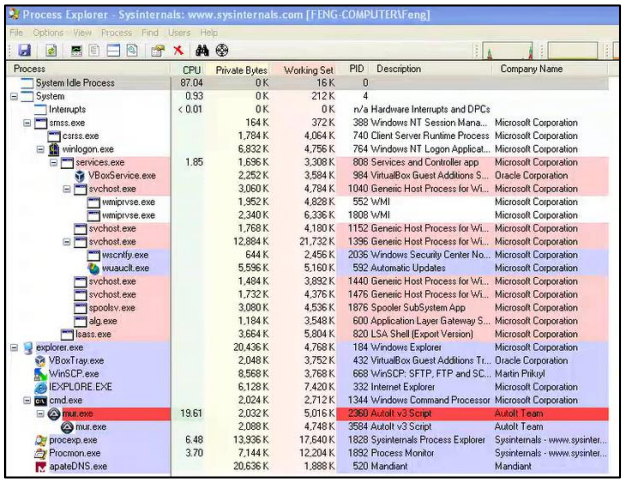
→ Mur.exe

→ Reg.Scvs ---(1)

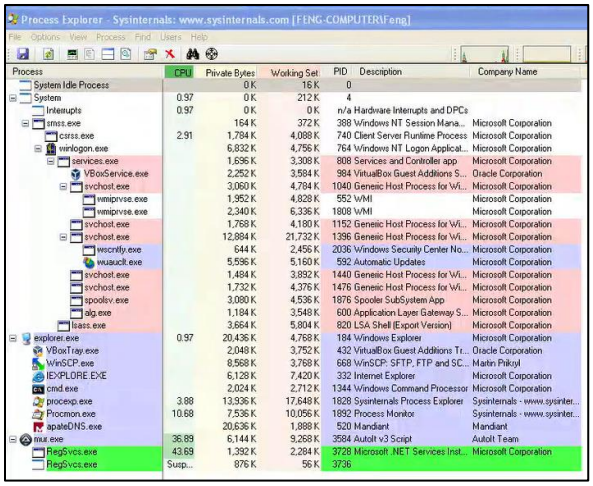
→ Reg.Scvs ---(2)

- The 1st mur.exe creates a 2nd mur.exe and terminates itself as seen below-



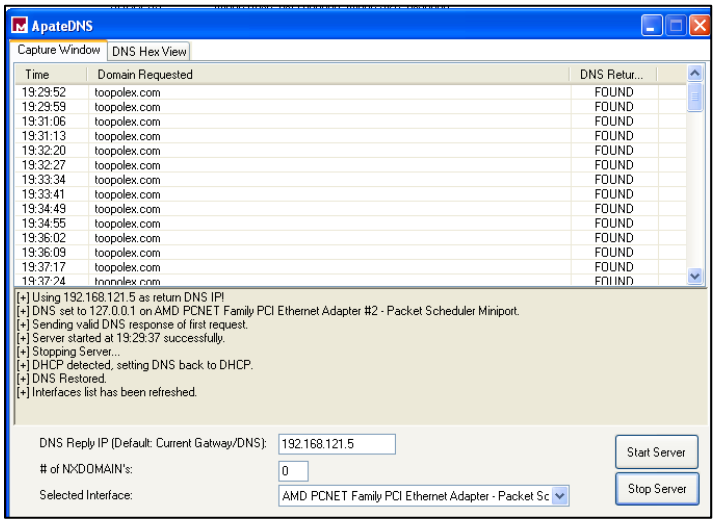


- Then, the 2nd mur.exe creates two new proceses called Reg.Svcs. It is observed that when the 2nd Reg.Svcs process is created, it is in suspended state for few seconds before becoming active.

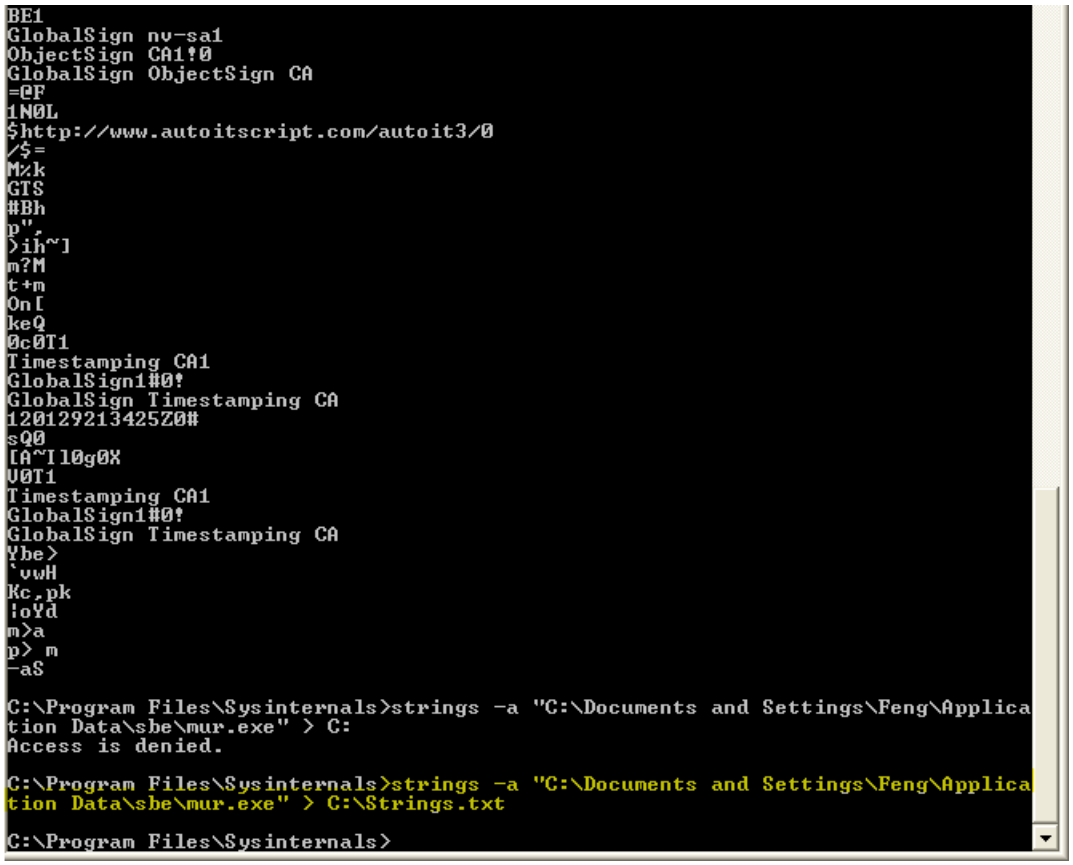


2. Domain name, exfiltrated strings

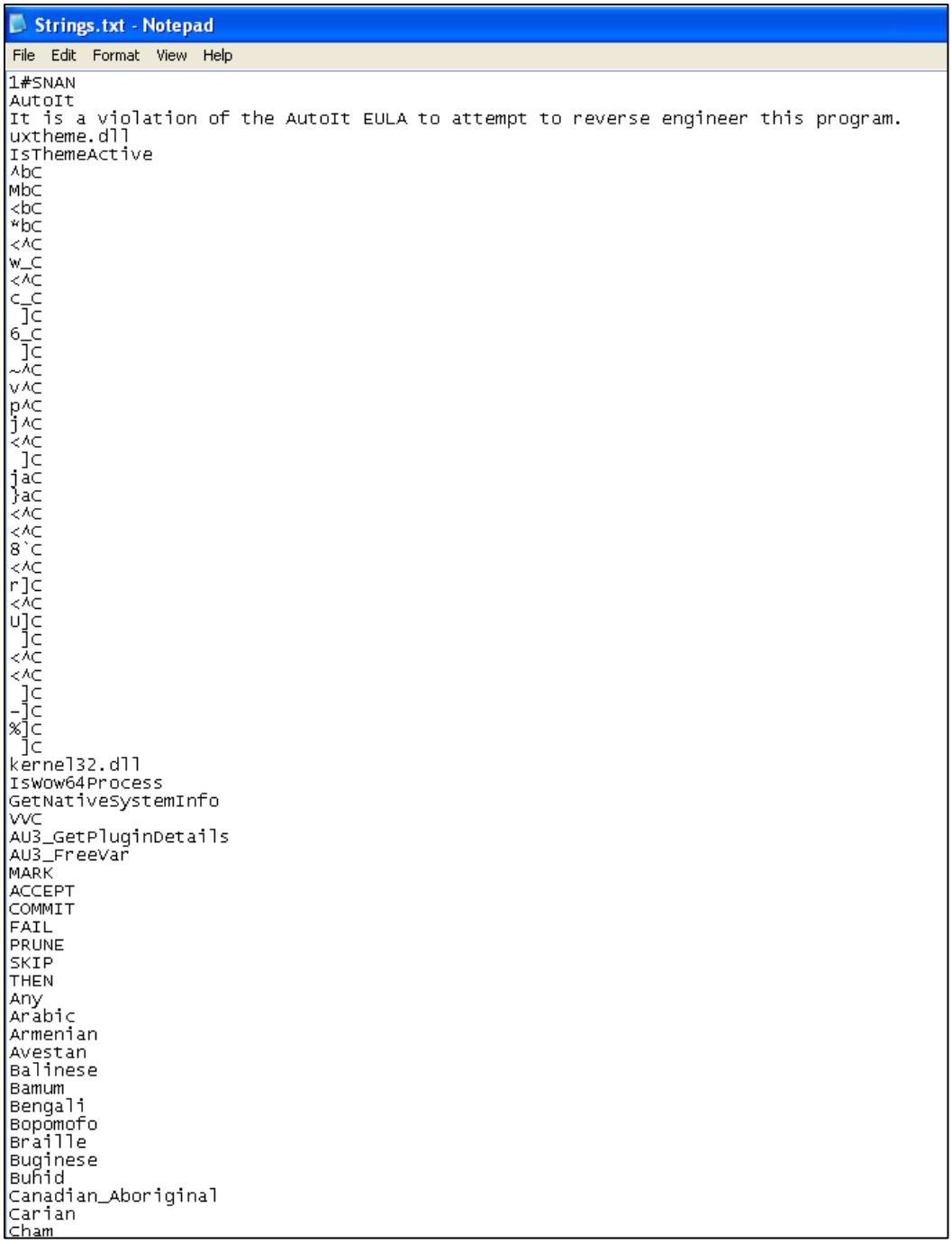
When the malware was executed from the command line as in above section, ApateDNS was set up to capture any possible network activity. It was observed that the malware communicates with the domain toopolex.com which is its command and control server.

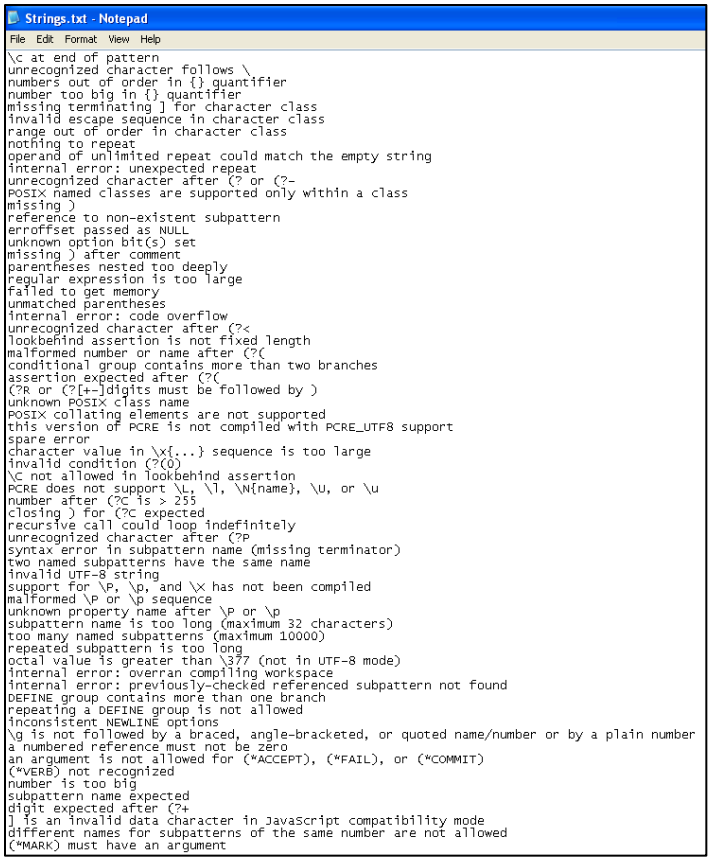


- Below is the screenshot of exfiltrated strings-


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~Il0g0X
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.txt - Notepad
File Edit Format View Help
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
_At
DZH
v)VW3
?~)V
G;{
tNh
F$S3


Strings.txt - Notepad
File Edit Format View Help
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



Strings.txt - Notepad

File Edit Format View Help

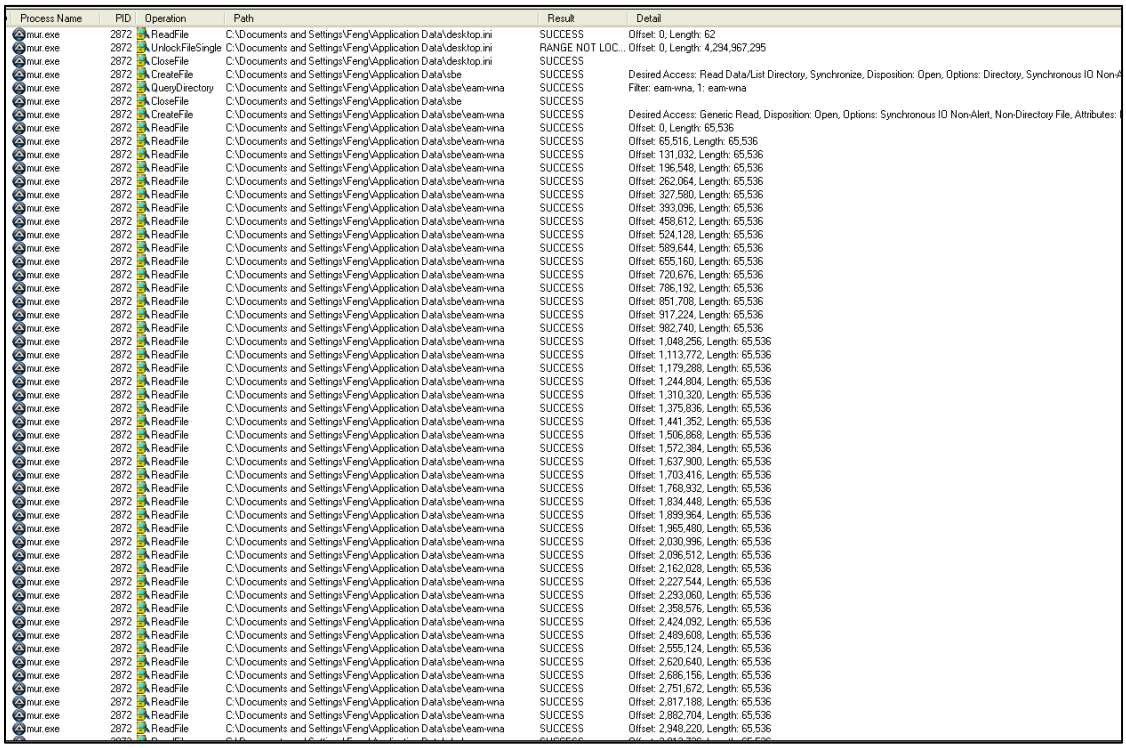
```
\c at end of pattern
unrecognized character follows \
numbers out of order in {} quantifier
number too big in {} quantifier
missing terminating ] for character class
invalid escape sequence in character class
range out of order in character class
nothing to repeat
operand of unlimited repeat could 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
```

RaiseException
MulDiv
GetVersionExW
GetSystemInfo
InterlockedIncrement
InterlockedDecrement
WideCharToMultiByte
lstrcpyW
MultiByteToWideChar
lstrlenW
lstrcmpiW
GetModuleHandleW
QueryPerformanceCounter
VirtualFreeEx
OpenProcess
VirtualAllocEx
WriteProcessMemory
ReadProcessMemory
CreateFileW
SetFilePointerEx
ReadFile
WriteFile
FlushFileBuffers
TerminateProcess
CreateToolhelp32Snapshot
Process32FirstW
Process32NextW
SetFileTime
GetFileAttributesW
FindFirstFileW
FindClose
DeleteFileW
FindNextFileW
MoveFileW
CopyFileW
CreateDirectoryW
RemoveDirectoryW
SetSystemPowerState
QueryPerformanceFrequency
FindResourceW
LoadResource
LockResource
SizeofResource
EnumResourceNamesW
OutputDebugStringW
GetLocalTime
CompareStringW
DeleteCriticalSection
EnterCriticalSection
LeaveCriticalSection

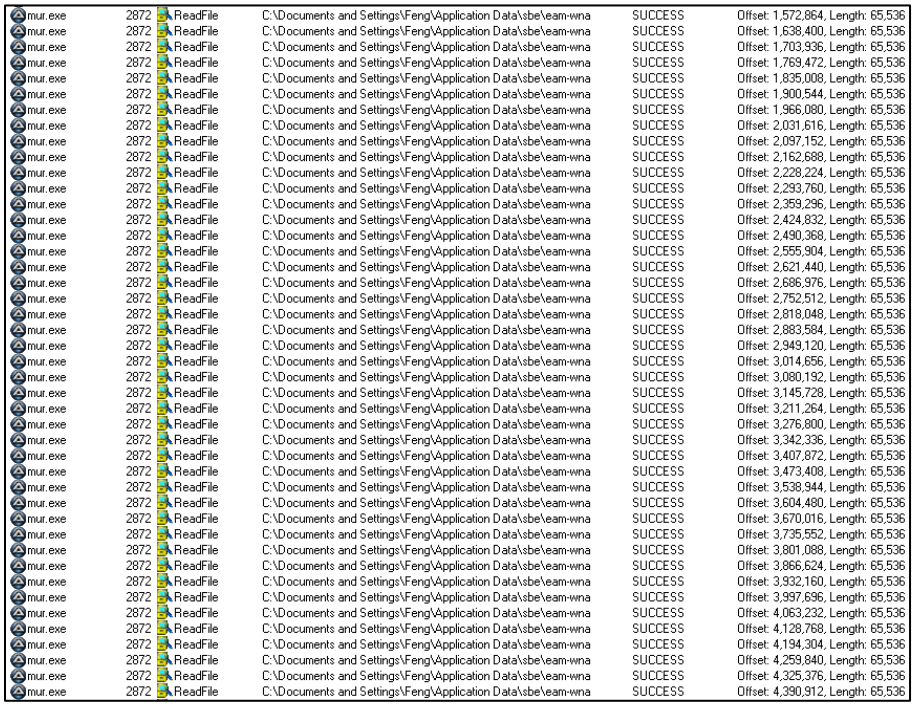
3. Analysis of 1st mur.exe

The PID of this process was captured using Process explorer and it was used as a filter to check the file and process activity using ProcMon.

- It was observed that this process reads extensively from eam-wna file as seen in below sreenshot.

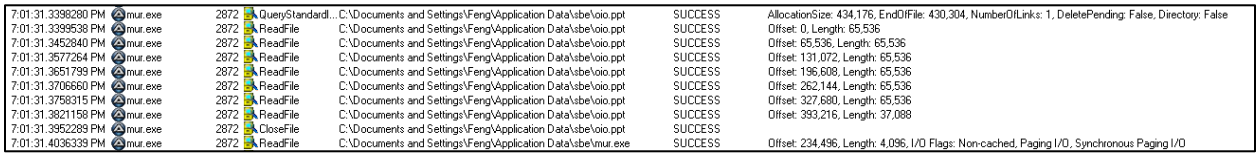


Process Name	PID	Operation	Path	Result	Detail
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\desktop.ini	SUCCESS	Offset: 0, Length: 62
mur.exe	2872	UnlockFileSingle	C:\Documents and Settings\Feng\Application Data\desktop.ini	RANGE NOT LOC...	Offset: 0, Length: 4,294,967,295
mur.exe	2872	CloseFile	C:\Documents and Settings\Feng\Application Data\desktop.ini	SUCCESS	
mur.exe	2872	CreateFile	C:\Documents and Settings\Feng\Application Data\sbe	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-A
mur.exe	2872	QueryDirectory	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Filter: eam-wna, 1: eam-wna
mur.exe	2872	CloseFile	C:\Documents and Settings\Feng\Application Data\sbe	SUCCESS	
mur.exe	2872	CreateFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes:
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 0, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 65,516, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 131,032, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 196,548, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 262,064, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 327,580, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 393,096, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 458,612, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 524,128, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 589,644, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 655,160, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 720,676, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 786,192, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 851,708, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 917,224, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 982,740, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,048,256, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,113,772, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,179,288, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,244,804, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,310,320, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,375,836, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,441,352, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,506,868, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,572,384, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,637,900, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,703,416, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,768,932, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,834,448, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,899,964, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,965,480, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,030,996, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,096,512, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,162,028, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,227,544, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,293,060, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,358,576, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,424,092, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,489,608, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,555,124, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,620,640, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,686,156, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,751,672, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,817,188, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,882,704, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,948,220, Length: 65,536



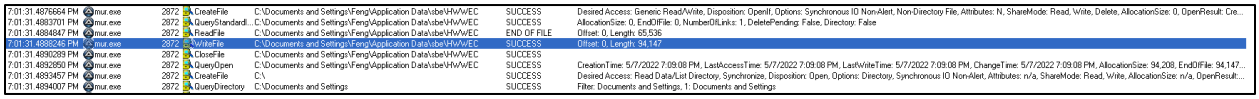
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,572,864, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,638,400, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,703,936, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,769,472, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,835,008, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,900,544, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 1,966,080, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,031,616, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,097,152, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,162,688, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,228,224, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,293,760, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,359,296, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,424,832, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,490,368, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,555,904, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,621,440, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,686,976, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,752,512, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,818,048, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,883,584, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 2,949,120, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 3,014,656, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 3,080,192, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 3,145,728, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 3,211,264, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 3,276,800, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 3,342,336, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 3,407,872, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 3,473,408, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 3,538,944, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 3,604,480, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 3,670,016, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 3,735,552, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 3,801,088, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 3,866,624, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 3,932,160, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 3,997,696, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 4,063,232, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 4,128,768, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 4,194,304, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 4,259,840, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 4,325,376, Length: 65,536
mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\eam-wna	SUCCESS	Offset: 4,390,912, Length: 65,536

- The process also reads file oio.ppt at different offesets from which we can infer that this is significant file used in malware execution.



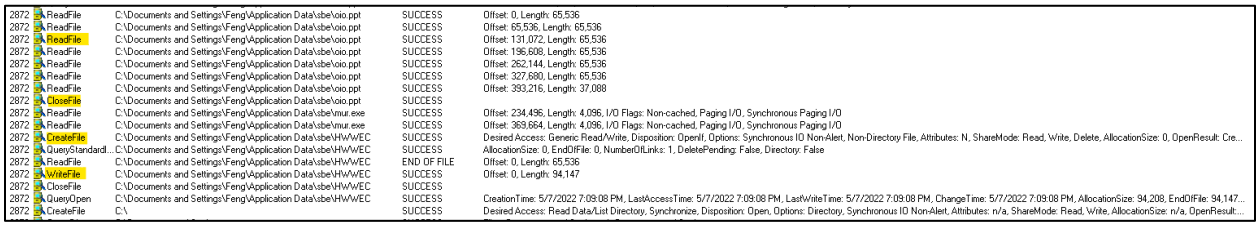
7:01:31.3398280 PM	mur.exe	2872	QueryStandardI...	C:\Documents and Settings\Feng\Application Data\sbe\oio.ppt	SUCCESS	AllocationSize: 434,176, EndOfFile: 430,304, NumberOfLinks: 1, DeletePending: False, Directory: False
7:01:31.3399538 PM	mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\oio.ppt	SUCCESS	Offset: 0, Length: 65,536
7:01:31.3452840 PM	mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\oio.ppt	SUCCESS	Offset: 65,536, Length: 65,536
7:01:31.3577264 PM	mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\oio.ppt	SUCCESS	Offset: 131,072, Length: 65,536
7:01:31.3651799 PM	mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\oio.ppt	SUCCESS	Offset: 196,608, Length: 65,536
7:01:31.3706660 PM	mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\oio.ppt	SUCCESS	Offset: 262,144, Length: 65,536
7:01:31.3758315 PM	mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\oio.ppt	SUCCESS	Offset: 327,680, Length: 65,536
7:01:31.3821158 PM	mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\oio.ppt	SUCCESS	Offset: 393,216, Length: 37,088
7:01:31.3952289 PM	mur.exe	2872	CloseFile	C:\Documents and Settings\Feng\Application Data\sbe\oio.ppt	SUCCESS	
7:01:31.4036339 PM	mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\mur.exe	SUCCESS	Offset: 234,496, Length: 4,096, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O

- A file was seen to be created with a random name, and WriteFile operation takes place to the file which means something is being written in this file, the length of which is 94,147 bytes. The temporary file name for this particular malware execution is HWWEC.



7:01:31.4876664 PM	mur.exe	2872	CreateFile	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	SUCCESS	Desired Access: Generic Read/Write, Disposition: OpenIf, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: 0, OpenResult: Cre...
7:01:31.4883701 PM	mur.exe	2872	QueryStandardI...	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	SUCCESS	AllocationSize: 0, EndOfFile: 0, NumberOfLinks: 1, DeletePending: False, Directory: False
7:01:31.4884847 PM	mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	END OF FILE	Offset: 0, Length: 65,536
7:01:31.4886245 PM	mur.exe	2872	WriteFile	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	SUCCESS	Offset: 0, Length: 94,147
7:01:31.4890289 PM	mur.exe	2872	CloseFile	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	SUCCESS	
7:01:31.4892850 PM	mur.exe	2872	QueryOpen	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	SUCCESS	CreationTime: 5/7/2022 7:09:08 PM, LastAccessTime: 5/7/2022 7:09:08 PM, LastWriteTime: 5/7/2022 7:09:08 PM, ChangeTime: 5/7/2022 7:09:08 PM, AllocationSize: 94,208, EndOfFile: 94,147...
7:01:31.4893457 PM	mur.exe	2872	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, AllocationSize: n/a, OpenResult:...
7:01:31.4894007 PM	mur.exe	2872	QueryDirectory	C:\Documents and Settings	SUCCESS	Filter: Documents and Settings, 1: Documents and Settings

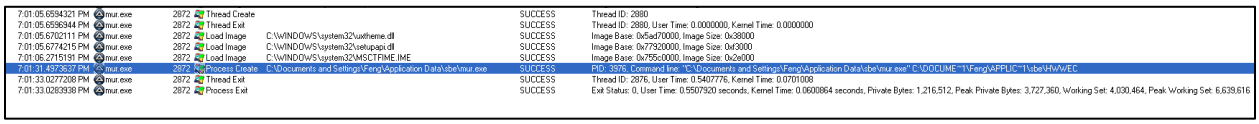
- Looking at the chronology of the File Activity, it can be suspected that the data that is being written in the temporary file, is the result of the read operations and possibly subsequent calculations carried out by the malware.



2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\oio.ppt	SUCCESS	Offset: 0, Length: 65,536
2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\oio.ppt	SUCCESS	Offset: 65,536, Length: 65,536
2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\oio.ppt	SUCCESS	Offset: 131,072, Length: 65,536
2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\oio.ppt	SUCCESS	Offset: 196,608, Length: 65,536
2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\oio.ppt	SUCCESS	Offset: 262,144, Length: 65,536
2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\oio.ppt	SUCCESS	Offset: 327,680, Length: 65,536
2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\oio.ppt	SUCCESS	Offset: 393,216, Length: 37,088
2872	CloseFile	C:\Documents and Settings\Feng\Application Data\sbe\oio.ppt	SUCCESS	
2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\mur.exe	SUCCESS	Offset: 234,496, Length: 4,096, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O
2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\mur.exe	SUCCESS	Offset: 369,664, Length: 4,096, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O
2872	CreateFile	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	SUCCESS	Desired Access: Generic Read/Write, Disposition: OpenIf, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: 0, OpenResult: Cre...
2872	QueryStandardI...	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	SUCCESS	AllocationSize: 0, EndOfFile: 0, NumberOfLinks: 1, DeletePending: False, Directory: False
2872	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	END OF FILE	Offset: 0, Length: 65,536
2872	WriteFile	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	SUCCESS	Offset: 0, Length: 94,147
2872	CloseFile	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	SUCCESS	
2872	QueryOpen	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	SUCCESS	CreationTime: 5/7/2022 7:09:08 PM, LastAccessTime: 5/7/2022 7:09:08 PM, LastWriteTime: 5/7/2022 7:09:08 PM, ChangeTime: 5/7/2022 7:09:08 PM, AllocationSize: 94,208, EndOfFile: 94,147...
2872	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, AllocationSize: n/a, OpenResult:...

- This process is responsible for spawning a child process called **mur.exe** using the commandline as highlighted in the screenshot below. Looking at the commandline, we can conclude that the 1st mur.exe uses the above generated file to launch the 2nd mur.exe.

The 2nd mur.exe takes the file created by the 1st mur.exe as commandline argument. When checked if that file was still present or not in the directory, it was not found which means it was a temporary file and most probably it had been deleted.



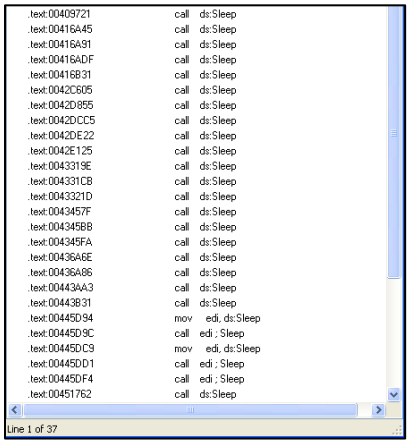
7:01:05.6594321 PM	mur.exe	2872	Thread Create		SUCCESS	Thread ID: 2880
7:01:05.6596944 PM	mur.exe	2872	Thread Exit		SUCCESS	Thread ID: 2880, User Time: 0.0000000, Kernel Time: 0.0000000
7:01:05.6702111 PM	mur.exe	2872	Load Image	C:\WINDOWS\system32\uxtheme.dll	SUCCESS	Image Base: 0x5ad70000, Image Size: 0x38000
7:01:05.6774215 PM	mur.exe	2872	Load Image	C:\WINDOWS\system32\setupapi.dll	SUCCESS	Image Base: 0x77920000, Image Size: 0xf3000
7:01:06.2715191 PM	mur.exe	2872	Load Image	C:\WINDOWS\system32\MSCTFIME.IME	SUCCESS	Image Base: 0x755c0000, Image Size: 0x2e000
7:01:31.4978637 PM	mur.exe	2872	Process Create	C:\Documents and Settings\Feng\Application Data\sbe\mur.exe	SUCCESS	PID: 3976, Command line: "C:\Documents and Settings\Feng\Application Data\sbe\mur.exe" C:\DOCUME~1\Feng\APPLIC~1\sbe\HWWEC
7:01:33.0277208 PM	mur.exe	2872	Thread Exit		SUCCESS	Thread ID: 2876, User Time: 0.5407776, Kernel Time: 0.0701008
7:01:33.0283938 PM	mur.exe	2872	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.5507920 seconds, Kernel Time: 0.0600864 seconds, Private Bytes: 1,216,512, Peak Private Bytes: 3,727,360, Working Set: 4,030,464, Peak Working Set: 6,639,616

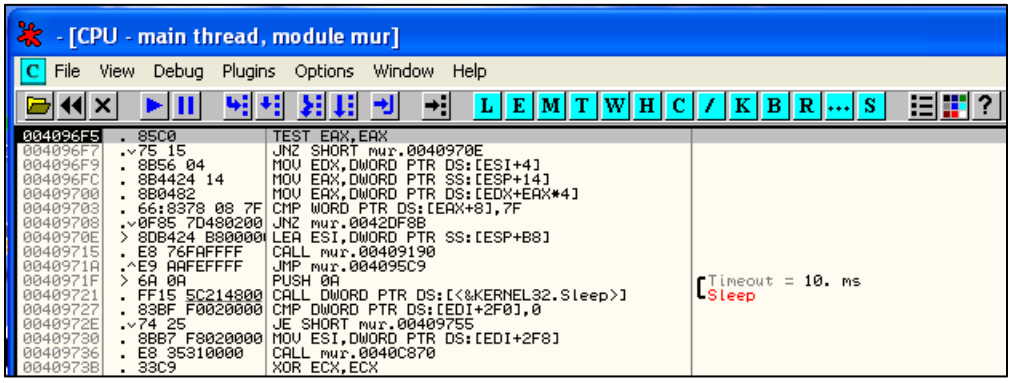
The above commandline sets the difference between the 1st mur.exe and 2nd mur.exe as the command line for each is different and hence they have a different behaviour.

The mur.exe executable itself does not change. This was verified by checking the hash value of the execuatble before and after running the malware. And they were found to be same.

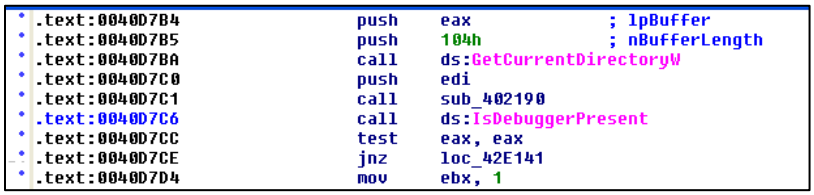
- Few Anti-debugging/Sandbox evasion techniques were found while debugging the code, starting with setting the break point at CreateProcessW

1. Many instances were found where Sleep API was called – This function is usually used for sandbox evasion. By delaying its execution beyond this timeframe malware can hide its malicious actions and activities from the sandbox. As a result of this, some malware has evolved to detect these patches as an additional indicator of an analysis/sandbox environment. This is done by taking a timestamp, going to sleep, and checking the timestamp upon waking up. If the time difference from the previously taken timestamp is substantially different than the time the malware was programmed to sleep, the malware will avoid or adjust its execution.





2. Also, a couple of instances were found where IsDebuggerPresent API was called – It is perhaps the simplest anti-debugging method. This function detects if the calling process is being debugged by a user-mode debugger. If the current process is running in the context of a debugger, the return value is nonzero.



```
00421EB7 . C705 70714900 MOV DWORD PTR DS:[497170],C0000409
00421EC1 . C705 74714900 MOV DWORD PTR DS:[497174],1
00421ECB . A1 400D4900   MOV EAX,DWORD PTR DS:[490D40]
00421ED0 . 8985 D8FCFFFF MOV DWORD PTR SS:[EBP-328],EAX
00421ED6 . A1 440D4900   MOV EAX,DWORD PTR DS:[490D44]
00421EDB . 8985 DCFCFFFF MOV DWORD PTR SS:[EBP-324],EAX
00421EE1 . FF15 2C234800 CALL DWORD PTR DS:[<&KERNEL32.IsDebuggerPresent>]   CIsDebuggerPresent
00421EE7 . A3 C0714900   MOV DWORD PTR DS:[4971C0],EAX
00421EEC . 6A 01         PUSH 1
00421EEE . E8 46DEFFFF   CALL mur.0041FD39
00421EF3 . 59            POP ECX
00421EF4 . 6A 00         PUSH 0                                              CpTopLevelFilter = NULL
00421EF6 . FF15 84234800 CALL DWORD PTR DS:[<&KERNEL32.SetUnhandledExceptionFilter>]  CSetUnhandledExceptionFilter
00421EFC . 68 DC434800   PUSH mur.004843DC                                   CpExceptionInfo = mur.004843DC
00421F01 . FF15 80234800 CALL DWORD PTR DS:[<&KERNEL32.UnhandledExceptionFilter>]  CUnhandledExceptionFilter
00421F07 . 833D C0714900 CMP DWORD PTR DS:[4971C0],0
```

- This process also supports the functionality to shutdown / reboot the system. It uses many different APIs for this purpose such as:

1. InitiateSystemShutDownExW

```
.text:00433427 ; ---------------------------------------------------------------------------
.text:00433427
.text:00433427 loc_433427:                             ; CODE XREF: sub_4333A3+74↑j
.text:00433427                 xor     ecx, ecx
.text:00433429                 test    bl, 14h
.text:0043342C                 jz      short loc_433433
.text:0043342E                 mov     ecx, 1
.text:00433433
.text:00433433 loc_433433:                             ; CODE XREF: sub_4333A3+89↑j
.text:00433433                 xor     eax, eax
.text:00433435                 test    bl, 2
.text:00433438                 jz      short loc_43343F
.text:0043343A                 mov     eax, 1
.text:0043343F
.text:0043343F loc_43343F:                             ; CODE XREF: sub_4333A3+95↑j
.text:0043343F                 mov     edx, [ebp+arg_4]
.text:00433442                 push    edx
.text:00433443                 push    eax
.text:00433444                 push    ecx
.text:00433445                 push    0
.text:00433447                 push    0
.text:00433449                 push    0
.text:0043344B                 call    ds:InitiateSystemShutdownExW
.text:00433451                 pop     ebx
.text:00433452                 mov     esp, ebp
.text:00433454                 pop     ebp
.text:00433455                 retn
.text:00433456 ; ---------------------------------------------------------------------------
```

2. SetSystemPowerState

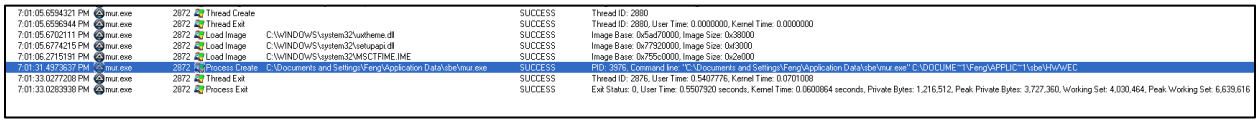
```
; ---------------------------------------------------------------------------

loc_433456:                            ; CODE XREF: sub_4333A3+6A↑j
                mov     eax, 1
                push    0               ; fForce
                push    eax             ; fSuspend
                call    ds:SetSystemPowerState
                pop     ebx
                mov     esp, ebp
                pop     ebp
                retn
; ---------------------------------------------------------------------------

loc_433469:                            ; CODE XREF: sub_4333A3+6F↑j
                xor     eax, eax
                push    eax             ; fForce
                push    eax             ; fSuspend
                call    ds:SetSystemPowerState
                pop     ebx
                mov     esp, ebp
                pop     ebp
                retn
sub_4333A3      endp
```

3. ExitWindowsEx

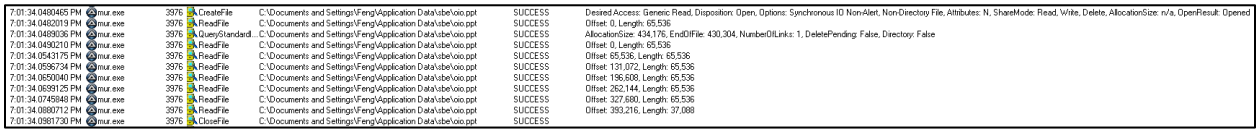
```
.text:0043340A ; ---------------------------------------------------------------------------
.text:0043340A
.text:0043340A loc_43340A:                             ; CODE XREF: sub_4333A3+5E↑j
.text:0043340A                 cmp     ebx, 20h
.text:0043340D                 jz      short loc_433456
.text:0043340F                 cmp     ebx, 40h
.text:00433412                 jz      short loc_433469
.text:00433414                 test    bl, 08h
.text:00433417                 jnz     short loc_433427
.text:00433419                 push    0               ; dwReserved
.text:0043341B                 push    ebx             ; uFlags
.text:0043341C                 call    ds:ExitWindowsEx ; Logoff/Restart/Shut down
.text:00433422                 pop     ebx
.text:00433423                 mov     esp, ebp
.text:00433425                 pop     ebp
.text:00433426                 retn
.text:00433427 ; ---------------------------------------------------------------------------
```

4. Analysis of 2st mur.exe

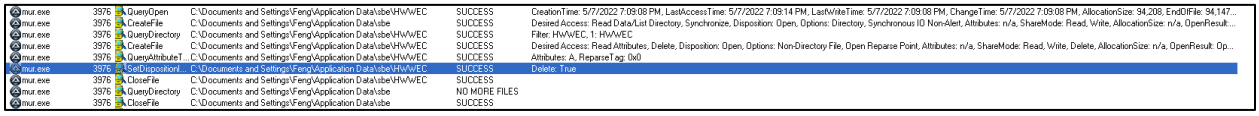
In reference to the child process created by 1st mur.exe as seen in below screenshot, the PID of this child process was applied as filter in Process Monitor for further analysis.



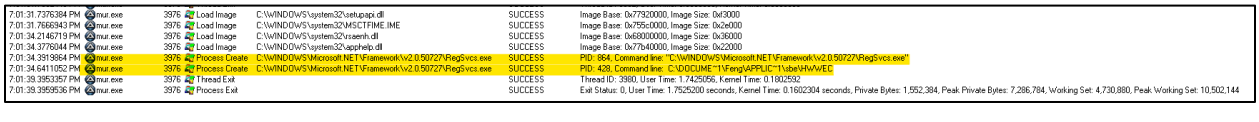
-It was seen that this process reads extensively from mur.exe which probably could be its parent process. Also, it reads many offsets from oio.ppt file



- The temporary file created HWWEC does not exist anymore in the directory as it could have been deleted. To confirm this, FileActivity tab of ProcessMonitor was explored and it was found that the file was indeed deleted.



- It was observed that this process spawns two other processes with name Reg.Svcs using different command lines as highlighted in below screenshot. The 1st Reg.Svcs uses the same temporary file that was used launch the 2nd mur.exe process.

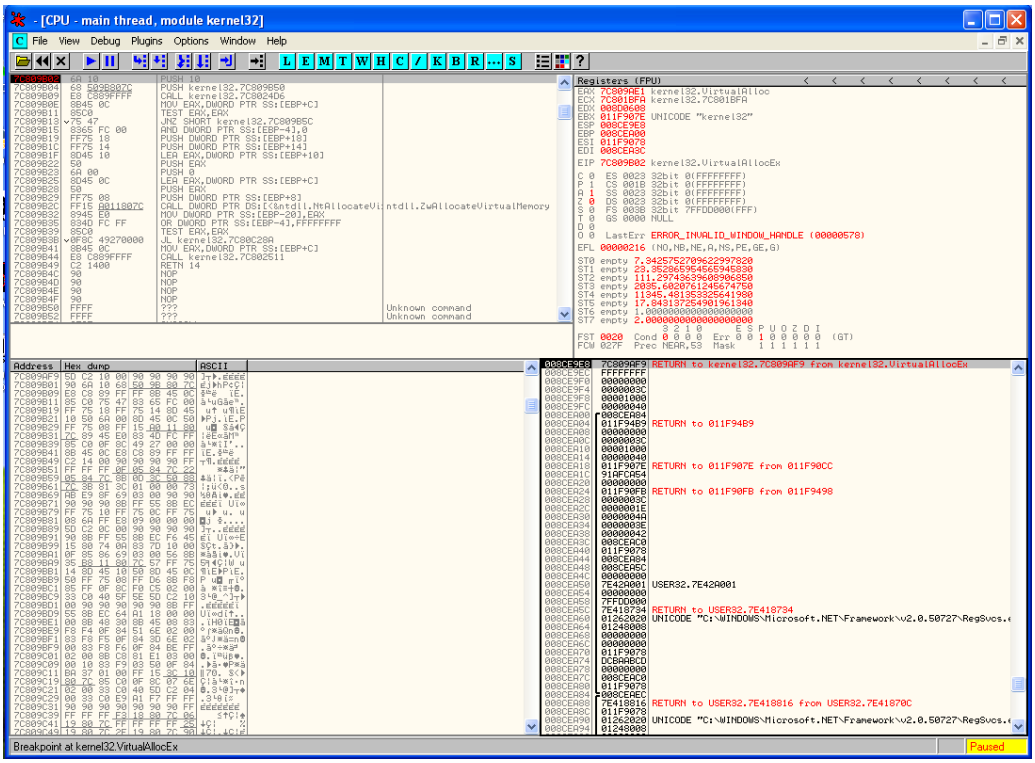


- This process is involved in process replacement or process hollowing. It occurs when a malware unmaps (hollows out) the legitimate code from memory of the target process, and overwrites the memory space of the target process (e.g., svchost.exe) with a malicious executable.

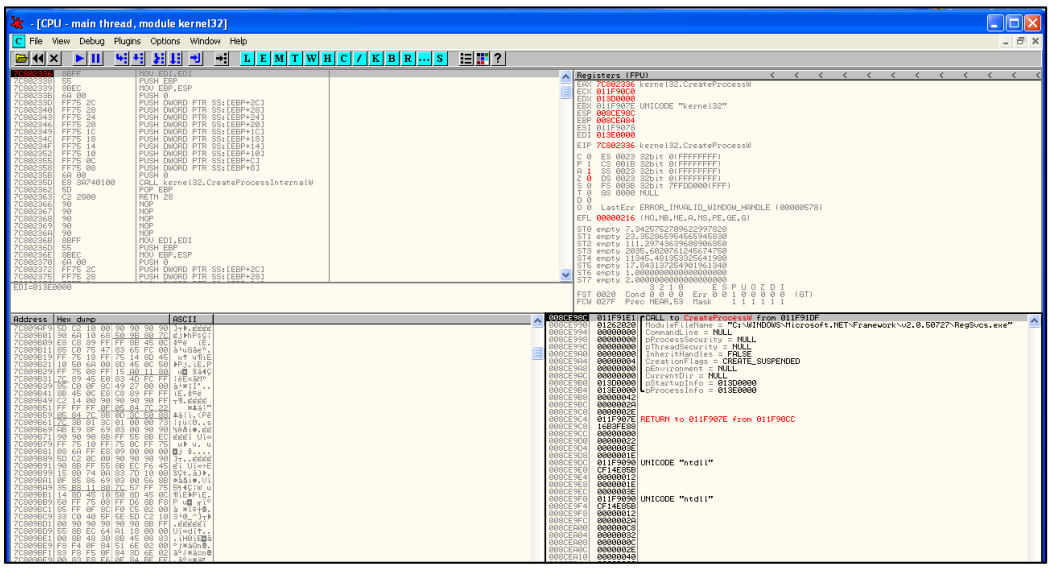
Following are steps that shows the evidence.

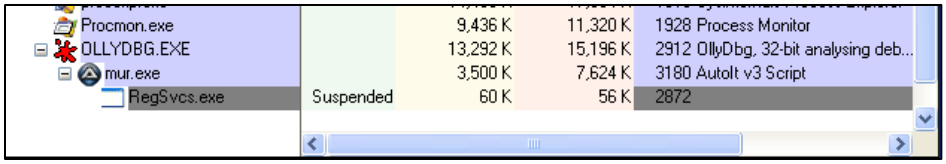
Using Ollydbg, breakpoint was set at CreateProcessW, WriteProcessMemory, GetThreatContext, SetThreatContext, VirtualAllocEx.

1- Virtual Allocation of memory takes places for the creation of the process.

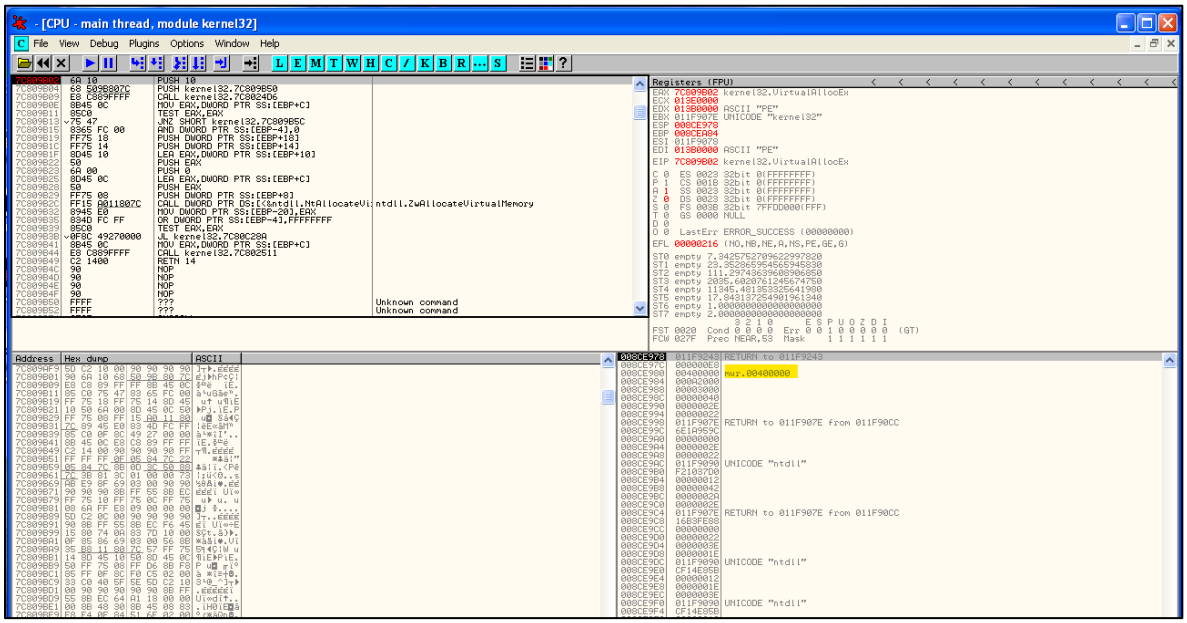


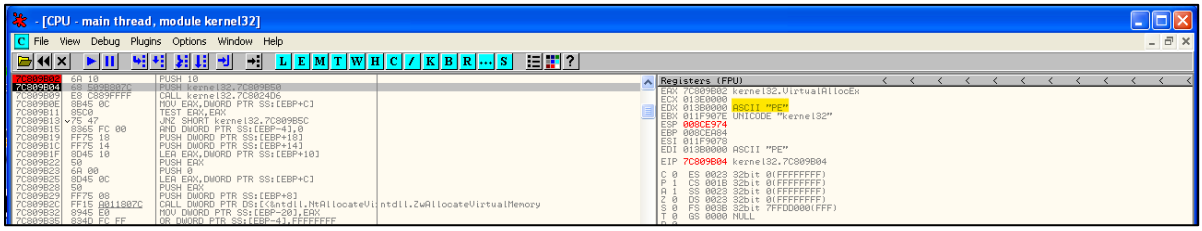
2. Now, the Reg.svcs process is created in the suspended state.



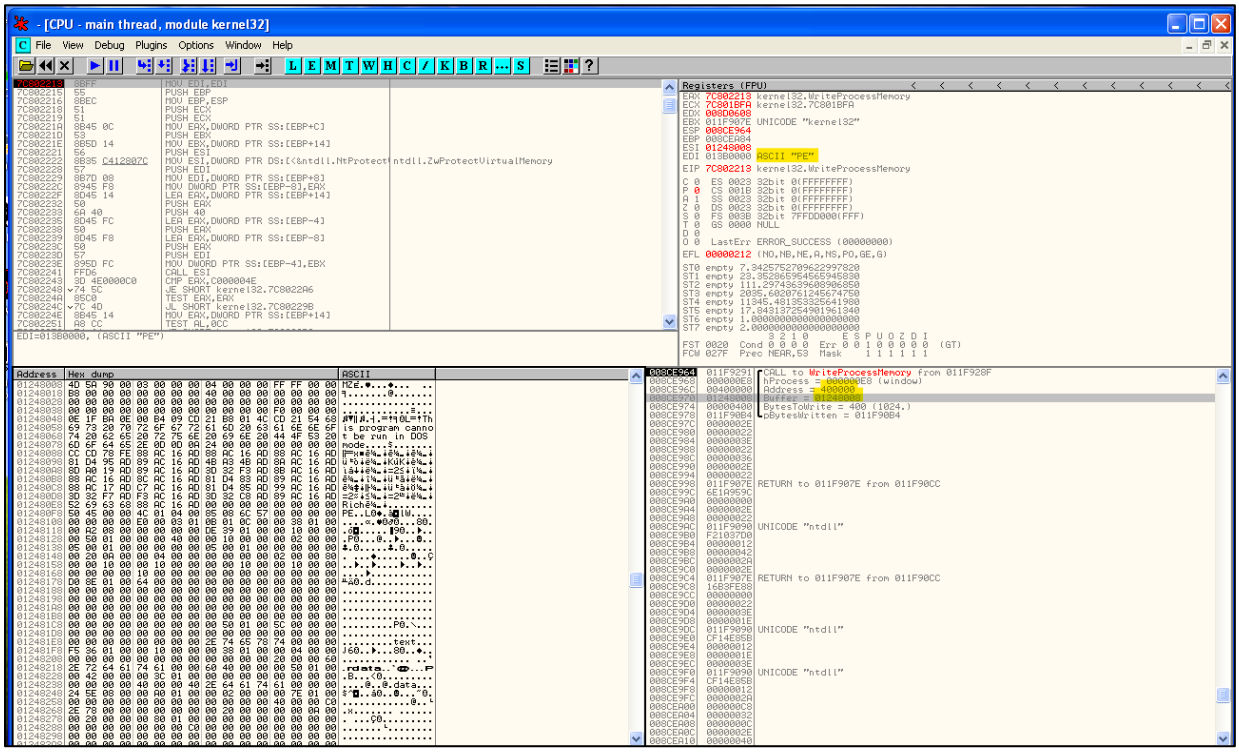


3. Again the virtul allocation of memory takes place, but this time it is for the malware executable.

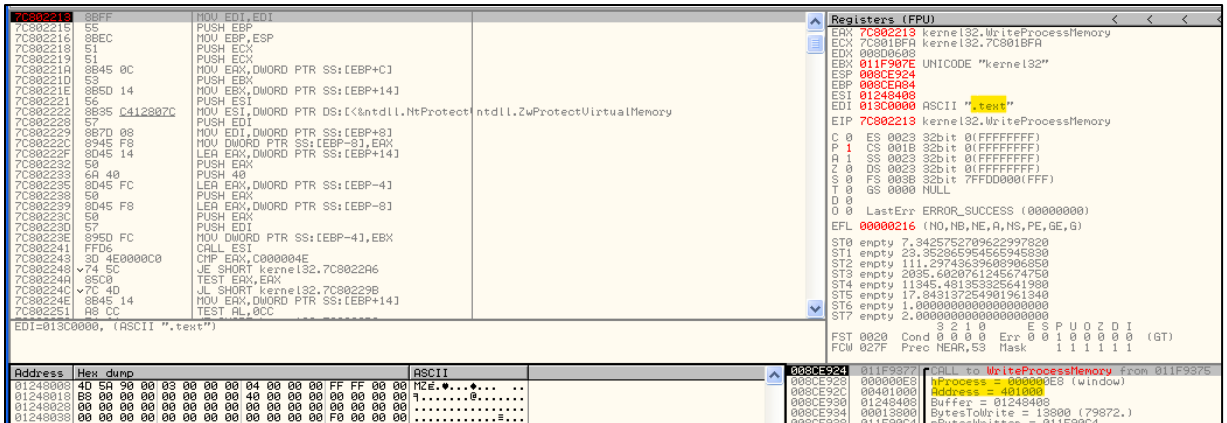


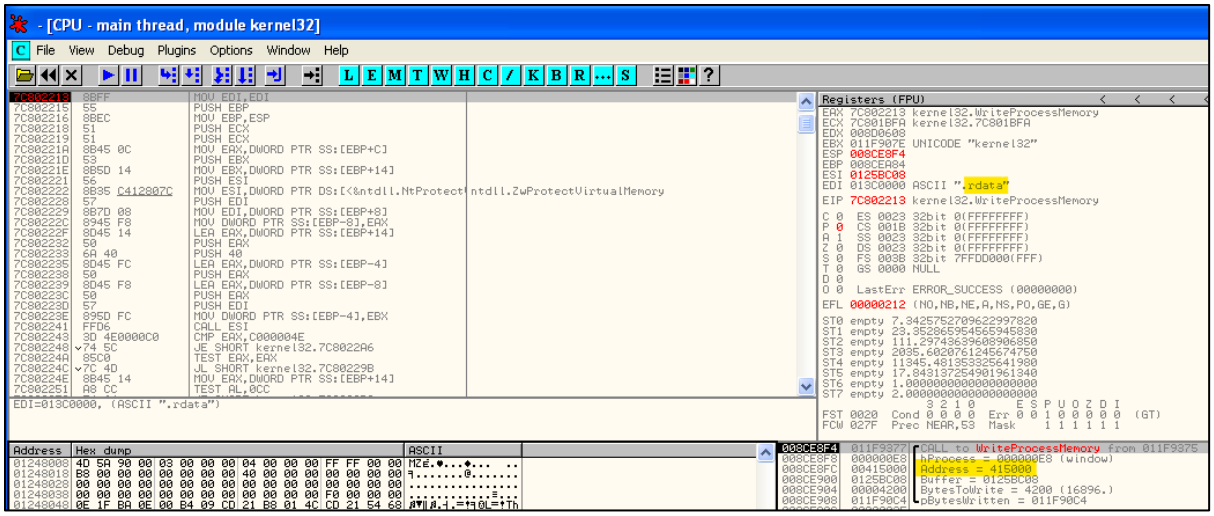


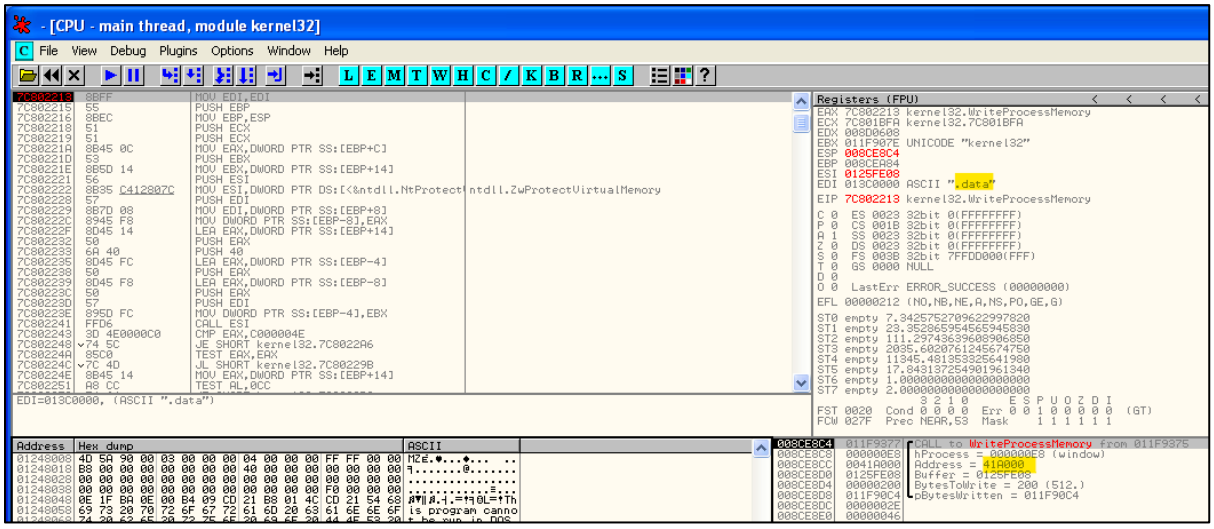
4. Now, the WriteProcessMemory function is executed. Here, the Address is the start of RAM for the Reg.Svcs process and the buffer contains the PE file. Below is the output of the buffer if we follow it in dump.

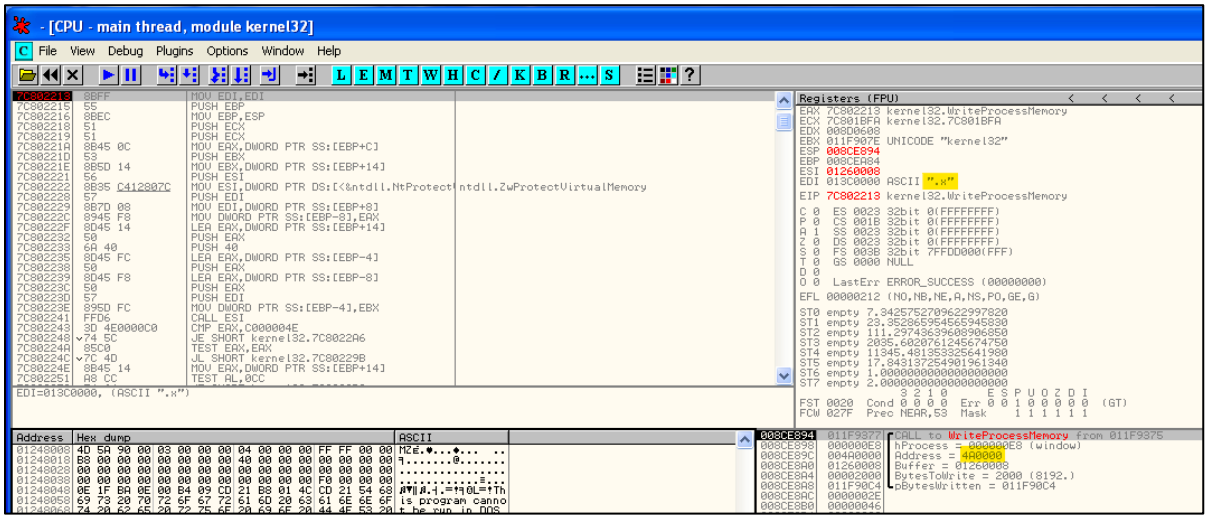


It was observed that this function executes multiple times and in each execution, it writes each section of the malware executable at the given address.

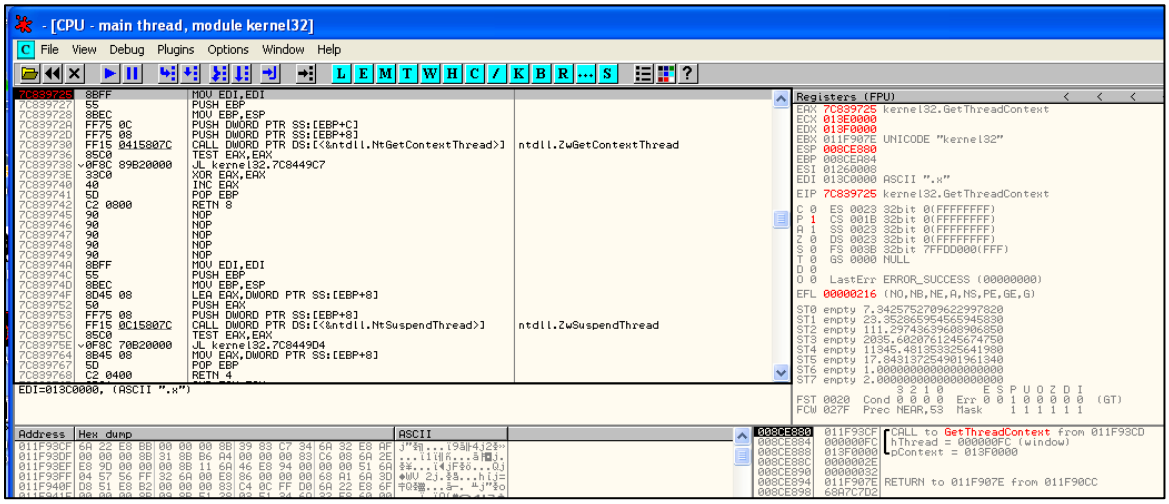



- [CPU - main thread, module kernel32]
File View Debug Plugins Options Window Help
7C802213 8BFF MOV EDI,EDI
7C802215 55 PUSH EBP
7C802216 8BEC MOV EBP,ESP
7C802218 51 PUSH ECX
7C802219 51 PUSH ECX
7C80221A 8B45 0C MOV EAX,DWORD PTR SS:[EBP+C]
7C80221D 53 PUSH EBX
7C80221E 8B5D 14 MOV EBX,DWORD PTR SS:[EBP+14]
7C802221 56 PUSH ESI
7C802222 8B35 C412807C MOV ESI,DWORD PTR DS:[<&ntdll.NtProtect ntdll.ZwProtectVirtualMemory
7C802228 57 PUSH EDI
7C802229 8B7D 08 MOV EDI,DWORD PTR SS:[EBP+8]
7C80222C 8945 F8 MOV DWORD PTR SS:[EBP-8],EAX
7C80222F 8D45 14 LEA EAX,DWORD PTR SS:[EBP+14]
7C802232 50 PUSH EAX
7C802233 6A 40 PUSH 40
7C802235 8D45 FC LEA EAX,DWORD PTR SS:[EBP-4]
7C802238 50 PUSH EAX
7C802239 8D45 F8 LEA EAX,DWORD PTR SS:[EBP-8]
7C80223C 50 PUSH EAX
7C80223D 57 PUSH EDI
7C80223E 895D FC MOV DWORD PTR SS:[EBP-4],EBX
7C802241 FFD6 CALL ESI
7C802243 3D 4E0000C0 CMP EAX,C000004E
7C802248 74 5C JE SHORT kernel32.7C8022A6
7C80224A 85C0 TEST EAX,EAX
7C80224C 7C 4D JL SHORT kernel32.7C80229B
7C80224E 8B45 14 MOV EAX,DWORD PTR SS:[EBP+14]
7C802251 A8 CC TEST AL,0CC
EDI=013C0000, (ASCII ".rdata")
Registers (FPU)
EAX 7C802213 kernel32.WriteProcessMemory
ECX 7C801BFA kernel32.7C801BFA
EDX 008D0608
EBX 011F907E UNICODE "kernel32"
ESP 008CE8F4
EBP 008CEA84
ESI 0125BC08
EDI 013C0000 ASCII ".rdata"
EIP 7C802213 kernel32.WriteProcessMemory
C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 1 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000212 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty 7.3425752709622997820
ST1 empty 23.352865954565945830
ST2 empty 111.297436396089068850
ST3 empty 2035.6020761245674750
ST4 empty 11345.481353325641980
ST5 empty 17.843137254901961340
ST6 empty 1.000000000000000000
ST7 empty 2.000000000000000000
3 2 1 0 E S P U O Z D I
FST 0020 Cond 0 0 0 0 Err 0 0 1 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
Address Hex dump ASCII
01248008 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZÉ.♥...♦... ..
01248018 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ¸.......@.......
01248028 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01248038 00 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00 ....≡...
01248048 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ♫▼║♫.┤.=↑↑0L=↑Th
008CE8F4 011F9377 CALL to WriteProcessMemory from 011F9375
008CE8F8 000000E8 hProcess = 000000E8 (window)
008CE8FC 00415000 Address = 415000
008CE900 0125BC08 Buffer = 0125BC08
008CE904 00004200 BytesToWrite = 4200 (16896.)
008CE908 011F90C4 pBytesWritten = 011F90C4

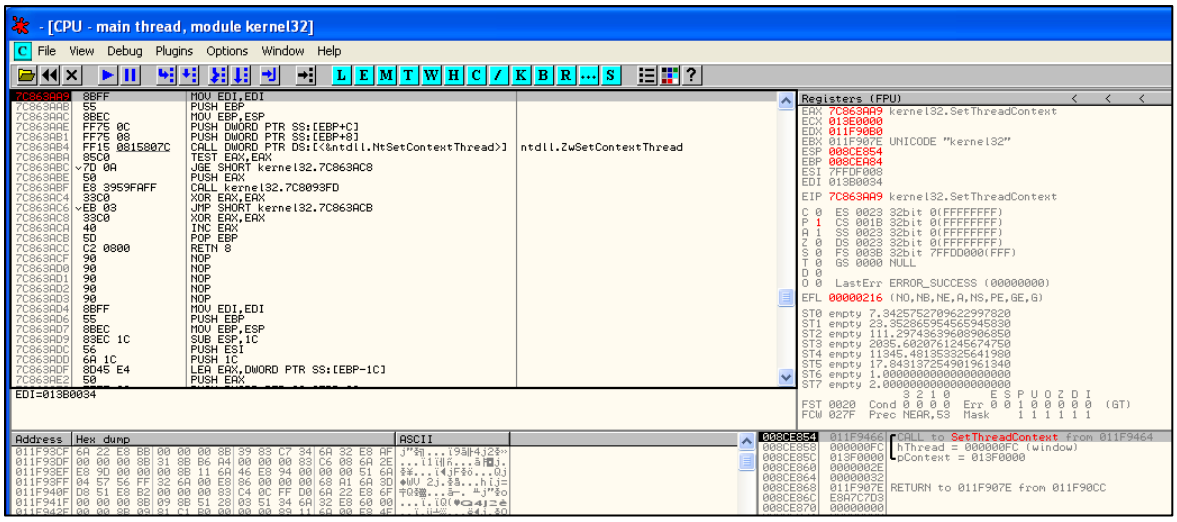

- [CPU - main thread, module kernel32]
File View Debug Plugins Options Window Help
7C802213 8BFF MOV EDI,EDI
7C802215 55 PUSH EBP
7C802216 8BEC MOV EBP,ESP
7C802218 51 PUSH ECX
7C802219 51 PUSH ECX
7C80221A 8B45 0C MOV EAX,DWORD PTR SS:[EBP+C]
7C80221D 53 PUSH EBX
7C80221E 8B5D 14 MOV EBX,DWORD PTR SS:[EBP+14]
7C802221 56 PUSH ESI
7C802222 8B35 C412807C MOV ESI,DWORD PTR DS:[<&ntdll.NtProtect ntdll.ZwProtectVirtualMemory
7C802228 57 PUSH EDI
7C802229 8B7D 08 MOV EDI,DWORD PTR SS:[EBP+8]
7C80222C 8945 F8 MOV DWORD PTR SS:[EBP-8],EAX
7C80222F 8D45 14 LEA EAX,DWORD PTR SS:[EBP+14]
7C802232 50 PUSH EAX
7C802233 6A 40 PUSH 40
7C802235 8D45 FC LEA EAX,DWORD PTR SS:[EBP-4]
7C802238 50 PUSH EAX
7C802239 8D45 F8 LEA EAX,DWORD PTR SS:[EBP-8]
7C80223C 50 PUSH EAX
7C80223D 57 PUSH EDI
7C80223E 895D FC MOV DWORD PTR SS:[EBP-4],EBX
7C802241 FFD6 CALL ESI
7C802243 3D 4E0000C0 CMP EAX,C000004E
7C802248 74 5C JE SHORT kernel32.7C8022A6
7C80224A 85C0 TEST EAX,EAX
7C80224C 7C 4D JL SHORT kernel32.7C80229B
7C80224E 8B45 14 MOV EAX,DWORD PTR SS:[EBP+14]
7C802251 A8 CC TEST AL,0CC
EDI=013C0000, (ASCII ".data")
Registers (FPU)
EAX 7C802213 kernel32.WriteProcessMemory
ECX 7C801BFA kernel32.7C801BFA
EDX 008D0608
EBX 011F907E UNICODE "kernel32"
ESP 008CE8C4
EBP 008CEA84
ESI 0125FE08
EDI 013C0000 ASCII ".data"
EIP 7C802213 kernel32.WriteProcessMemory
C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 1 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000212 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty 7.3425752709622997820
ST1 empty 23.352865954565945830
ST2 empty 111.297436396089068850
ST3 empty 2035.6020761245674750
ST4 empty 11345.481353325641980
ST5 empty 17.843137254901961340
ST6 empty 1.000000000000000000
ST7 empty 2.000000000000000000
3 2 1 0 E S P U O Z D I
FST 0020 Cond 0 0 0 0 Err 0 0 1 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
Address Hex dump ASCII
01248008 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZÉ.♥...♦... ..
01248018 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ¸.......@.......
01248028 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01248038 00 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00 ....≡...
01248048 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ♫▼║♫.┤.=↑↑0L=↑Th
01248058 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
008CE8C4 011F9377 CALL to WriteProcessMemory from 011F9375
008CE8C8 000000E8 hProcess = 000000E8 (window)
008CE8CC 0041A000 Address = 41A000
008CE8D0 0125FE08 Buffer = 0125FE08
008CE8D4 00000200 BytesToWrite = 200 (512.)
008CE8D8 011F90C4 pBytesWritten = 011F90C4
008CE8DC 0000002E
008CE8E0 00000046


- [CPU - main thread, module kernel32]
File View Debug Plugins Options Window Help
7C802213 8BFF MOV EDI,EDI
7C802215 55 PUSH EBP
7C802216 8BEC MOV EBP,ESP
7C802218 51 PUSH ECX
7C802219 51 PUSH ECX
7C80221A 8B45 0C MOV EAX,DWORD PTR SS:[EBP+C]
7C80221D 53 PUSH EBX
7C80221E 8B5D 14 MOV EBX,DWORD PTR SS:[EBP+14]
7C802221 56 PUSH ESI
7C802222 8B35 C412807C MOV ESI,DWORD PTR DS:[<&ntdll.NtProtect ntdll.ZwProtectVirtualMemory
7C802228 57 PUSH EDI
7C802229 8B7D 08 MOV EDI,DWORD PTR SS:[EBP+8]
7C80222C 8945 F8 MOV DWORD PTR SS:[EBP-8],EAX
7C80222F 8D45 14 LEA EAX,DWORD PTR SS:[EBP+14]
7C802232 50 PUSH EAX
7C802233 6A 40 PUSH 40
7C802235 8D45 FC LEA EAX,DWORD PTR SS:[EBP-4]
7C802238 50 PUSH EAX
7C802239 8D45 F8 LEA EAX,DWORD PTR SS:[EBP-8]
7C80223C 50 PUSH EAX
7C80223D 57 PUSH EDI
7C80223E 895D FC MOV DWORD PTR SS:[EBP-4],EBX
7C802241 FFD6 CALL ESI
7C802243 3D 4E0000C0 CMP EAX,C000004E
7C802248 74 5C JE SHORT kernel32.7C8022A6
7C80224A 85C0 TEST EAX,EAX
7C80224C 7C 4D JL SHORT kernel32.7C80229B
7C80224E 8B45 14 MOV EAX,DWORD PTR SS:[EBP+14]
7C802251 A8 CC TEST AL,0CC
EDI=013C0000, (ASCII ".x")
Registers (FPU)
EAX 7C802213 kernel32.WriteProcessMemory
ECX 7C801BFA kernel32.7C801BFA
EDX 008D0608
EBX 011F907E UNICODE "kernel32"
ESP 008CE894
EBP 008CEA84
ESI 01260008
EDI 013C0000 ASCII ".x"
EIP 7C802213 kernel32.WriteProcessMemory
C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 1 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000212 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty 7.3425752709622997820
ST1 empty 23.352865954565945830
ST2 empty 111.297436396089068850
ST3 empty 2035.6020761245674750
ST4 empty 11345.481353325641980
ST5 empty 17.843137254901961340
ST6 empty 1.000000000000000000
ST7 empty 2.000000000000000000
3 2 1 0 E S P U O Z D I
FST 0020 Cond 0 0 0 0 Err 0 0 1 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
Address Hex dump ASCII
01248008 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZÉ.♥...♦... ..
01248018 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ¸.......@.......
01248028 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01248038 00 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00 ....≡...
01248048 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ♫▼║♫.┤.=↑↑0L=↑Th
01248058 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
008CE894 011F9377 CALL to WriteProcessMemory from 011F9375
008CE898 000000E8 hProcess = 000000E8 (window)
008CE89C 004A0000 Address = 4A0000
008CE8A0 01260008 Buffer = 01260008
008CE8A4 00002000 BytesToWrite = 2000 (8192.)
008CE8A8 011F90C4 pBytesWritten = 011F90C4
008CE8AC 0000002E
008CE8B0 00000046

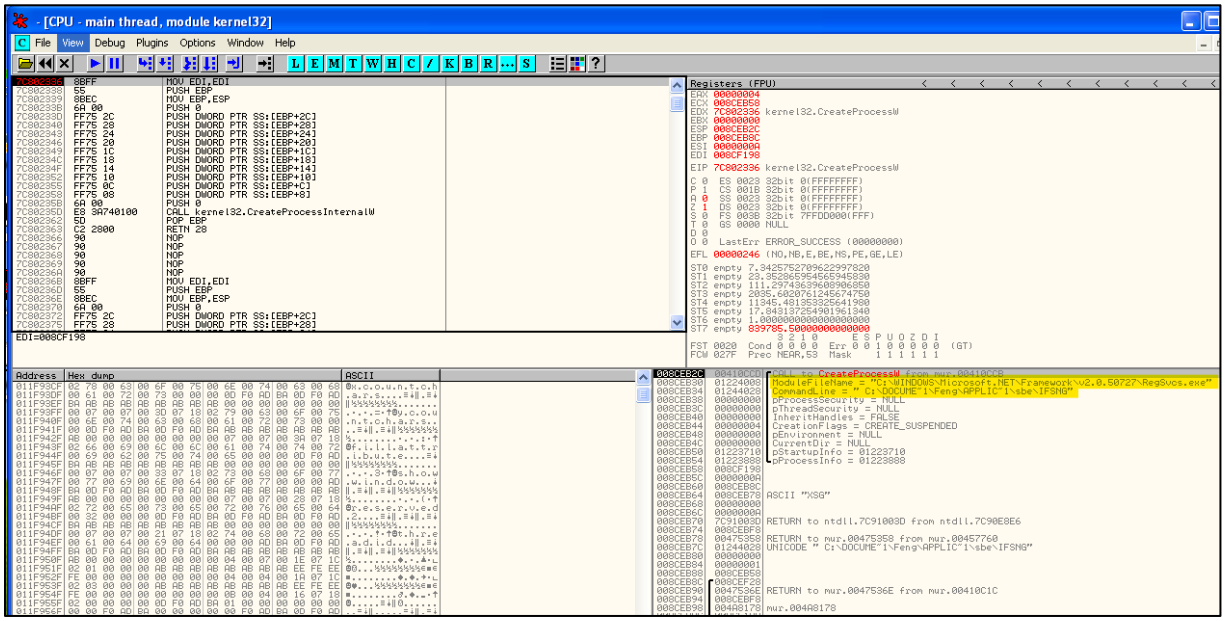
5. Next, GetThreatContext function is called to retrieve the thread context of the specified thread.



6. After this, SetThreadContext is executed to point the entrypoint to a new code section that it has written.



7. And Finally, the malicious Reg.svcs gets created whose command line has same temporary file name as that was used to launch the 2nd mur.exe.

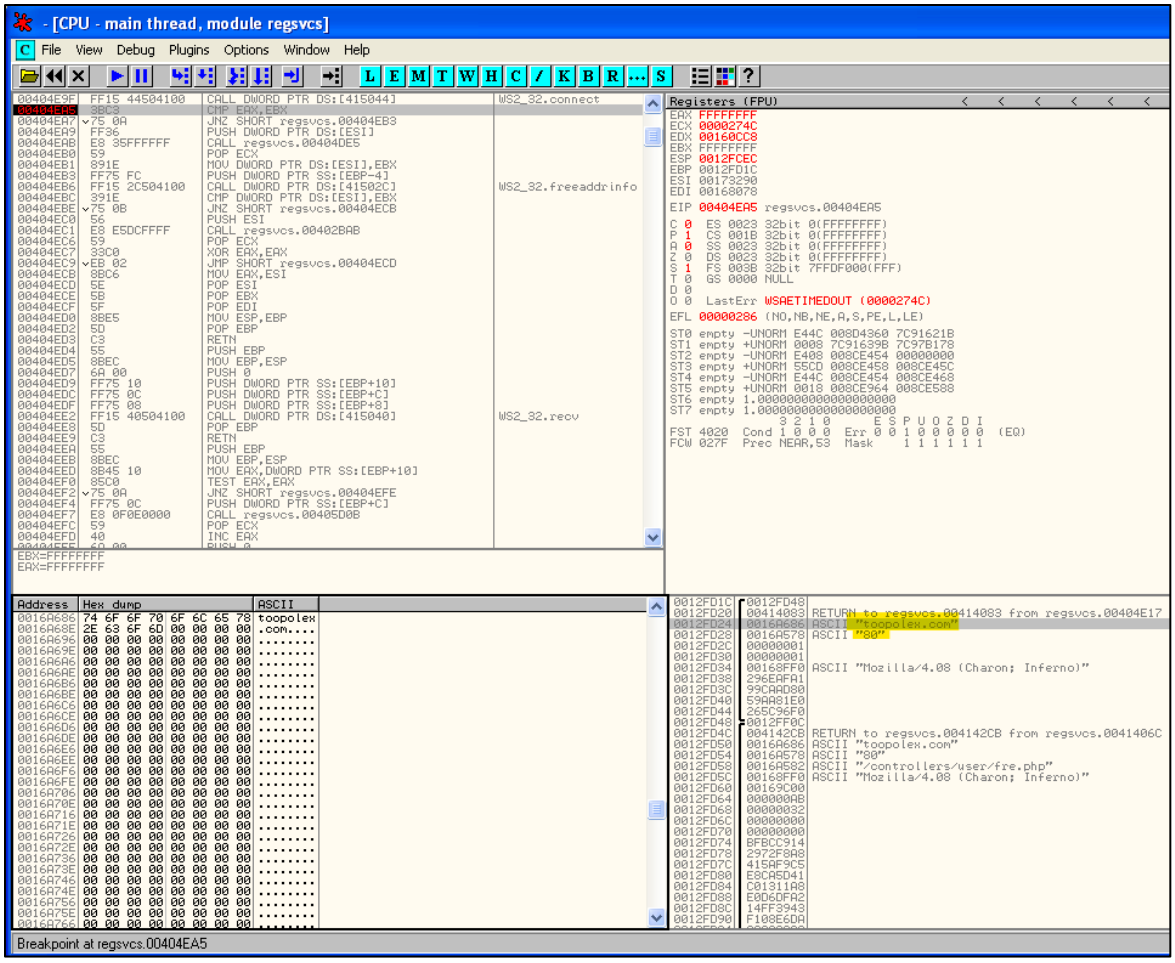


5. Analysis of 1st Reg.svcs Process

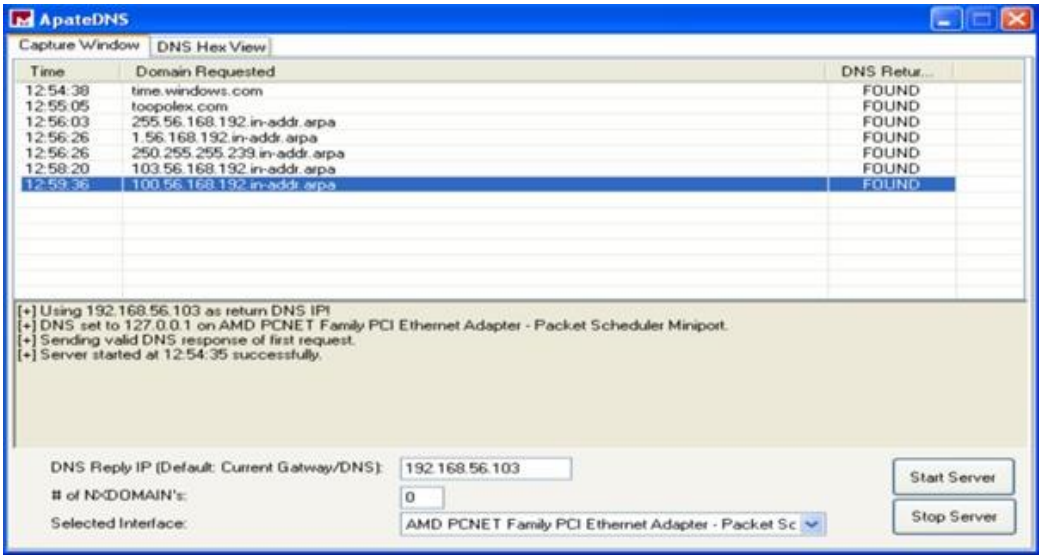
After this process was spawned by 2nd mur.exe, using the PID from process explorer, this executable's activity was looked upon from Process Monitor.

- From the Network tab, it can be concluded that this process is responsible for some kind of network activity.

- The domain it is getting connected to is tooplex.com. This was confirmed by setting a breakpoint at Ws32.connect API and following the stack from where it is called from to see the input arguments it taken in.

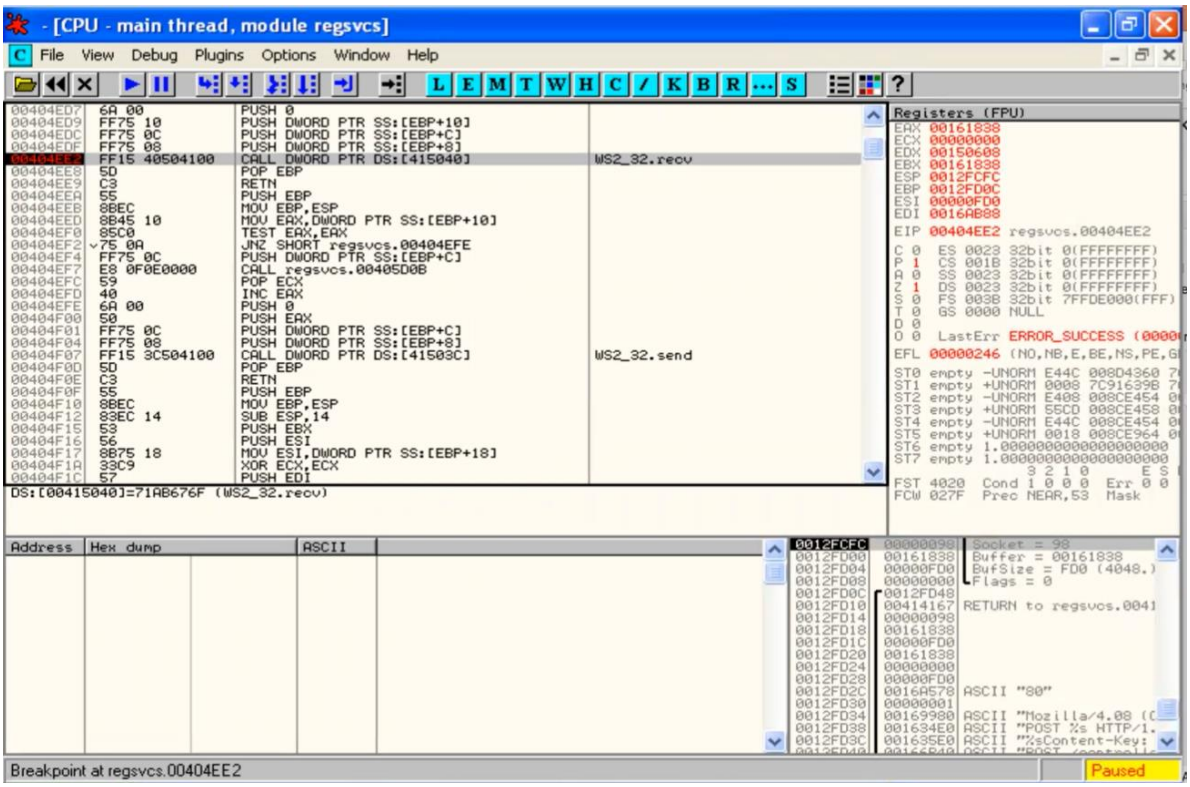


Also, it was observed that once internal gateway was set in ApateDNS, this process tries to establish a connection with other Ips along with toopolex.com domain. Possibly, when it finds that the DNS is not resolving, it tries to reach the hard coded IPs which are possibly present in the malware's executable.



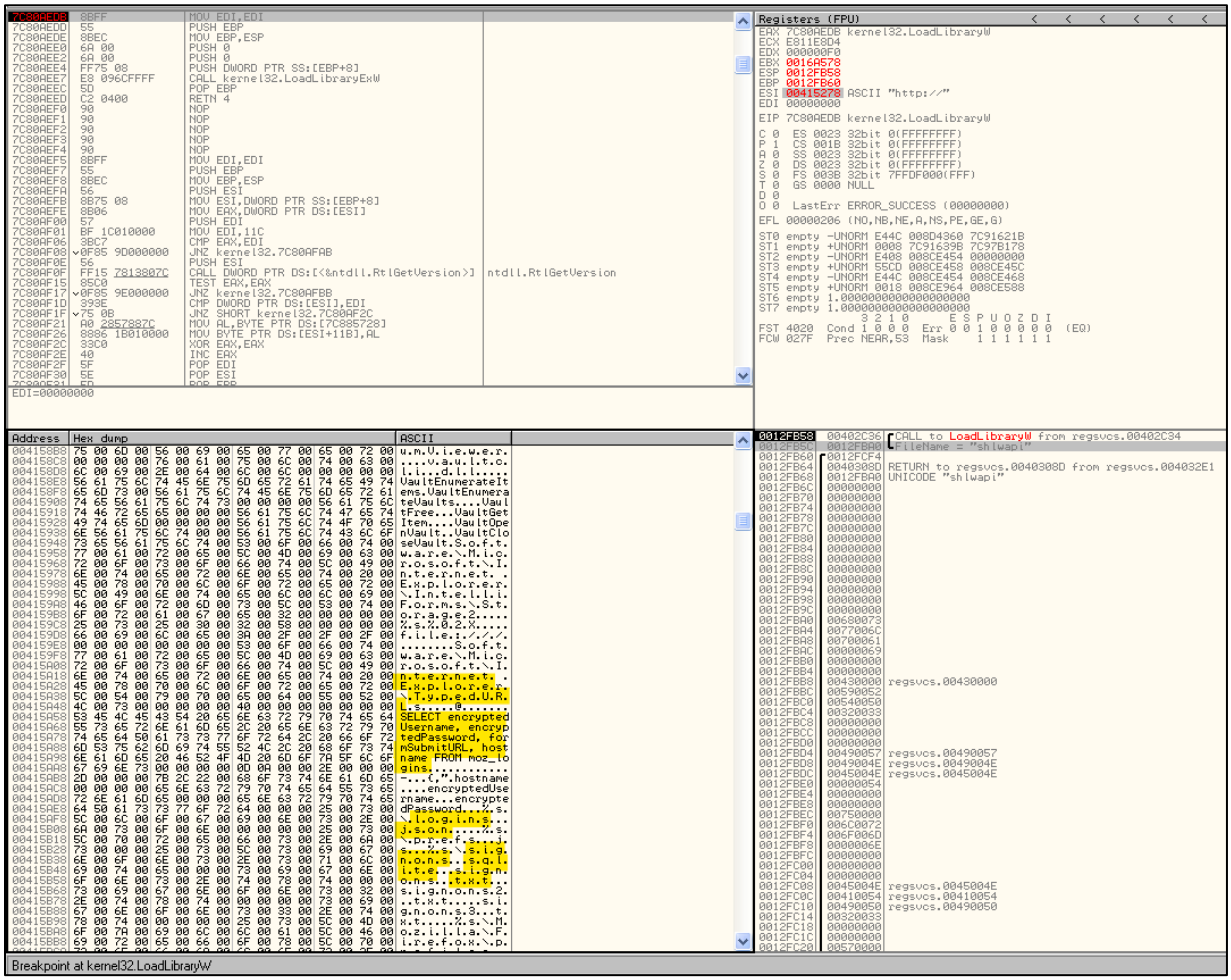
- Since, this process is involved in network activites, there would exist send and receive functions. In OllyDbg, breakpoints were set at these functions to observe the behaviour of the malware in little more detail. Below are some details-

Here, a breakpoint was set at receive function to see what the malware send to the netcat.



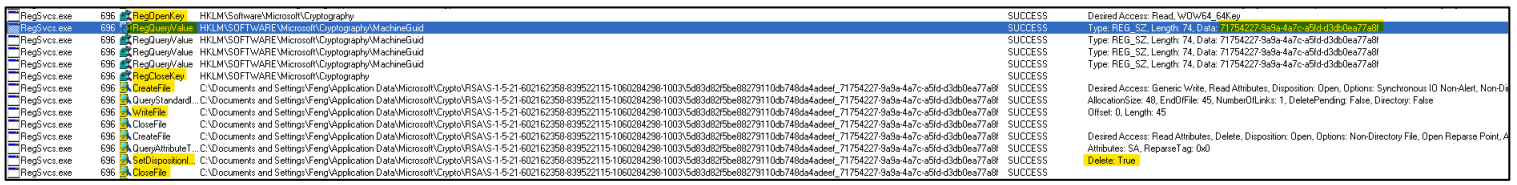
Below is the information that it sent to netcat which actually it would send to toopolex.com.

- Below highlighted SQL query and content such as %s logins.json, signons were found when the LoadLibraryW API was hit which hints that some kind of data exfiltration is taking place.



- This process was also found to be involved in information collection and data exfiltration. Below is screenshots of some data that is exfiltrated.

1. Cryptographic machine guid- Observing the chronology of below events, it looks like the process is reading the value of the registry key which is the Machine GUID, creating a temporary file and writing the data into it and later deleting the file and clearing tracks. This is how maybe the information is sent to the command and control server. – toopolex.com



2. Computer name- FENG COMPUTER

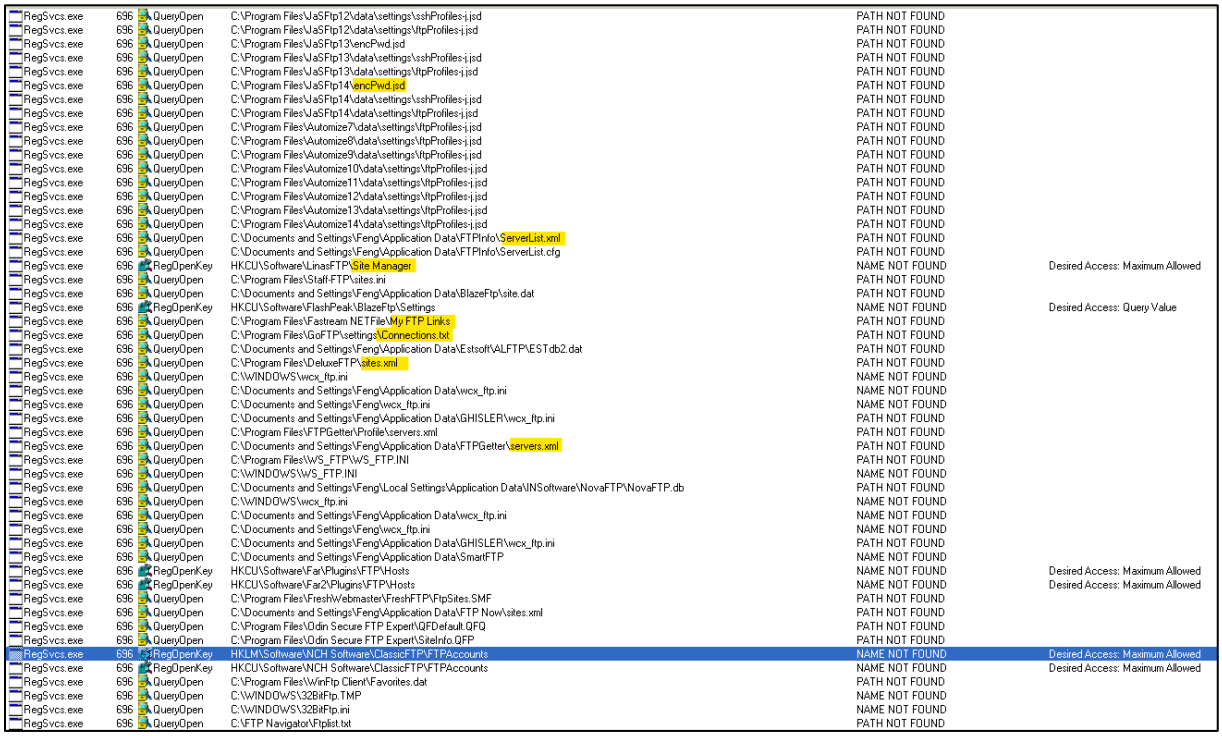
RegSvcs.exe	696	RegOpenKey	HKLM\System\CurrentControlSet\Control\ComputerName	SUCCESS	Desired Access: Read
RegSvcs.exe	696	RegOpenKey	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	SUCCESS	Desired Access: Read
RegSvcs.exe	696	RegQueryValue	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\ComputerName	SUCCESS	Type: REG_SZ, Length: 28, Data: FENG-COMPUTER
RegSvcs.exe	696	RegCloseKey	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	SUCCESS	
RegSvcs.exe	696	RegCloseKey	HKLM\System\CurrentControlSet\Control\ComputerName	SUCCESS	

3. Saved Credentials from applications-

a. As seen in the below screenshot, the process is querying to multiple applications and trying to read the login data.

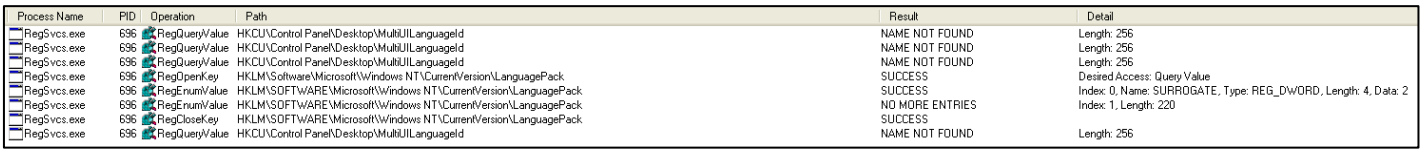
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data	SUCCESS
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Comodo\Dragon\User Data\Default\Web Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataComodo\Dragon\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataComodo\Dragon\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\MapleStudio\ChromePlus\User Data\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\MapleStudio\ChromePlus\User Data\Default\Web Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataMapleStudio\ChromePlus\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataMapleStudio\ChromePlus\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Google\Chrome\User Data\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Google\Chrome\User Data\Default\Web Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataGoogle\Chrome\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataGoogle\Chrome\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Nichrome\User Data\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Nichrome\User Data\Default\Web Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataNichrome\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataNichrome\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\RockMelt\User Data\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\RockMelt\User Data\Default\Web Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataRockMelt\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataRockMelt\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Spark\User Data\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Spark\User Data\Default\Web Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataSpark\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataSpark\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Chromium\User Data\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Chromium\User Data\Default\Web Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataChromium\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataChromium\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Titan Browser\User Data\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Titan Browser\User Data\Default\Web Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataTitan Browser\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataTitan Browser\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Torch\User Data\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Torch\User Data\Default\Web Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataTorch\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataTorch\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Yandex\YandexBrowser\User Data\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Yandex\YandexBrowser\User Data\Default\Web Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataYandex\YandexBrowser\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataYandex\YandexBrowser\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Epic Privacy Browser\User Data\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Epic Privacy Browser\User Data\Default\Web Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataEpic Privacy Browser\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataEpic Privacy Browser\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\CocCoc\Browser\User Data\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\CocCoc\Browser\User Data\Default\Web Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataCocCoc\Browser\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataCocCoc\Browser\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Vivaldi\User Data\Default\Login Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\Vivaldi\User Data\Default\Web Data	PATH NOT FOUND
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application DataVivaldi\Login Data	PATH NOT FOUND

b. Process is trying to read from all the below highlighted files related to FTP.



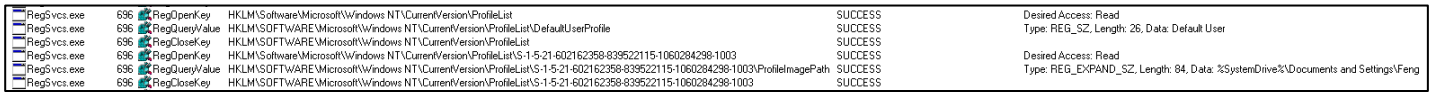
RegSvcs.exe	696	QueryOpen	C:\Program Files\UaSFtp12\data\settings\sshProfiles-j.jsd	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\UaSFtp12\data\settings\ftpProfiles-j.jsd	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\UaSFtp13\encPwd.jsd	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\UaSFtp13\data\settings\sshProfiles-j.jsd	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\UaSFtp13\data\settings\ftpProfiles-j.jsd	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\UaSFtp14\encPwd.jsd	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\UaSFtp14\data\settings\sshProfiles-j.jsd	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\UaSFtp14\data\settings\ftpProfiles-j.jsd	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\Automize7\data\settings\ftpProfiles-j.jsd	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\Automize8\data\settings\ftpProfiles-j.jsd	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\Automize9\data\settings\ftpProfiles-j.jsd	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\Automize10\data\settings\ftpProfiles-j.jsd	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\Automize11\data\settings\ftpProfiles-j.jsd	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\Automize12\data\settings\ftpProfiles-j.jsd	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\Automize13\data\settings\ftpProfiles-j.jsd	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\Automize14\data\settings\ftpProfiles-j.jsd	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\FTPInfo\ServerList.xml	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\FTPInfo\ServerList.cfg	PATH NOT FOUND	
RegSvcs.exe	696	RegOpenKey	HKCU\Software\LinasFTP\Site Manager	NAME NOT FOUND	Desired Access: Maximum Allowed
RegSvcs.exe	696	QueryOpen	C:\Program Files\Staff-FTP\sites.ini	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\BlazeFtp\site.dat	PATH NOT FOUND	
RegSvcs.exe	696	RegOpenKey	HKCU\Software\FlashPeak\BlazeFtp\Settings	NAME NOT FOUND	Desired Access: Query Value
RegSvcs.exe	696	QueryOpen	C:\Program Files\Fastream NETFile\My FTP Links	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\GoFTP\settings\Connections.txt	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\Estsoft\ALFTP\ESTdb2.dat	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\DeluxeFTP\sites.xml	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\WINDOWS\wcx_ftp.ini	NAME NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\wcx_ftp.ini	NAME NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\wcx_ftp.ini	NAME NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\GHISLER\wcx_ftp.ini	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\FTPGetter\Profile\servers.xml	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\FTPGetter\servers.xml	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\WS_FTP\WS_FTP.INI	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\WINDOWS\WS_FTP.INI	NAME NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\INSoftware\NovaFTP\NovaFTP.db	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\WINDOWS\wcx_ftp.ini	NAME NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\wcx_ftp.ini	NAME NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\wcx_ftp.ini	NAME NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\GHISLER\wcx_ftp.ini	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\SmartFTP	NAME NOT FOUND	
RegSvcs.exe	696	RegOpenKey	HKCU\Software\Far\Plugins\FTP\Hosts	NAME NOT FOUND	Desired Access: Maximum Allowed
RegSvcs.exe	696	RegOpenKey	HKCU\Software\Far2\Plugins\FTP\Hosts	NAME NOT FOUND	Desired Access: Maximum Allowed
RegSvcs.exe	696	QueryOpen	C:\Program Files\FreshWebmaster\FreshFTP\FtpSites.SMF	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\FTP Now\sites.xml	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\Odin Secure FTP Expert\QFDefault.QFQ	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\Program Files\Odin Secure FTP Expert\SiteInfo.QFP	PATH NOT FOUND	
RegSvcs.exe	696	RegOpenKey	HKLM\Software\NCH Software\ClassicFTP\FTPAccounts	NAME NOT FOUND	Desired Access: Maximum Allowed
RegSvcs.exe	696	RegOpenKey	HKCU\Software\NCH Software\ClassicFTP\FTPAccounts	NAME NOT FOUND	Desired Access: Maximum Allowed
RegSvcs.exe	696	QueryOpen	C:\Program Files\WinFtp Client\Favorites.dat	PATH NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\WINDOWS\32BitFtp.TMP	NAME NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\WINDOWS\32BitFtp.ini	NAME NOT FOUND	
RegSvcs.exe	696	QueryOpen	C:\FTP Navigator\Ftplist.txt	PATH NOT FOUND	

4. Reading System Language



Process Name	PID	Operation	Path	Result	Detail
RegSvcs.exe	696	RegQueryValue	HKCU\Control Panel\Desktop\MultiUILanguageId	NAME NOT FOUND	Length: 256
RegSvcs.exe	696	RegQueryValue	HKCU\Control Panel\Desktop\MultiUILanguageId	NAME NOT FOUND	Length: 256
RegSvcs.exe	696	RegQueryValue	HKCU\Control Panel\Desktop\MultiUILanguageId	NAME NOT FOUND	Length: 256
RegSvcs.exe	696	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\LanguagePack	SUCCESS	Desired Access: Query Value
RegSvcs.exe	696	RegEnumValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack	SUCCESS	Index: 0, Name: SURROGATE, Type: REG_DWORD, Length: 4, Data: 2
RegSvcs.exe	696	RegEnumValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack	NO MORE ENTRIES	Index: 1, Length: 220
RegSvcs.exe	696	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack	SUCCESS	
RegSvcs.exe	696	RegQueryValue	HKCU\Control Panel\Desktop\MultiUILanguageId	NAME NOT FOUND	Length: 256

5. ProfileLists



RegSvcs.exe	696	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList	SUCCESS	Desired Access: Read
RegSvcs.exe	696	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\DefaultUserProfile	SUCCESS	Type: REG_SZ, Length: 26, Data: Default User
RegSvcs.exe	696	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList	SUCCESS	
RegSvcs.exe	696	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-602162358-839522115-1060284298-1003	SUCCESS	Desired Access: Read
RegSvcs.exe	696	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-602162358-839522115-1060284298-1003\ProfileImagePath	SUCCESS	Type: REG_EXPAND_SZ, Length: 84, Data: %SystemDrive%\Documents and Settings\Feng
RegSvcs.exe	696	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-602162358-839522115-1060284298-1003	SUCCESS	

- There were encryption/encoding APIs found while debugging the process in OllyDbg which confirms that this process has this capability. Below were the APIs-

a. *CryptEncrypt* was found at 77DEE340. This accepts text or container data and returns container data as a binary file named encrypted.data

b. *CryptBinaryToStringA* was found at 77AB4020. This function converts an array of bytes into a formatted string.

- Apart from this, Keylogging APIs were also found while debugging in OllyDBG which confirms that this process has keylogging capabilities. Below were the APIs-

a. *GetAsyncKeyState* was found at 7E42A78F. This function gives information about the key, whether the key was pressed up or down at the time when the function is called. In simple words, it will check whether a key is pressed or not.

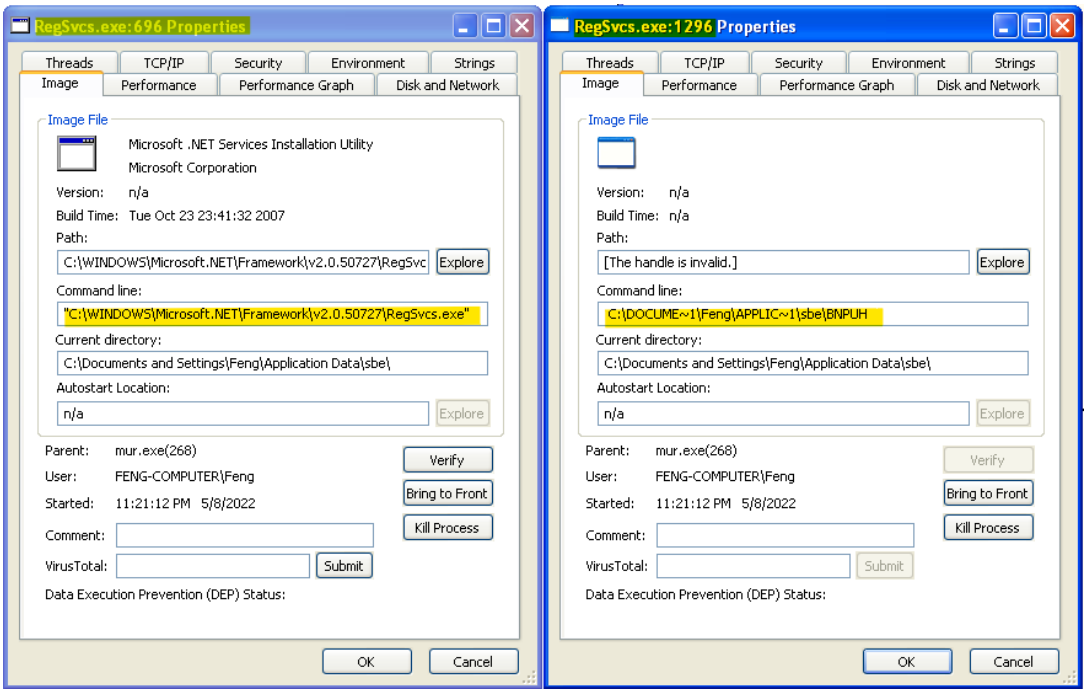
b. *GetWindowLongW* was found at 7E4188A6. This retrieves information about the specified window. The function also retrieves the 32-bit (DWORD) value at the specified offset into the extra window memory

c. *GetKeyState* was found at 7E429ED9. It checks if a keyboard key or mouse/joystick button is down or up. Also retrieves joystick status.

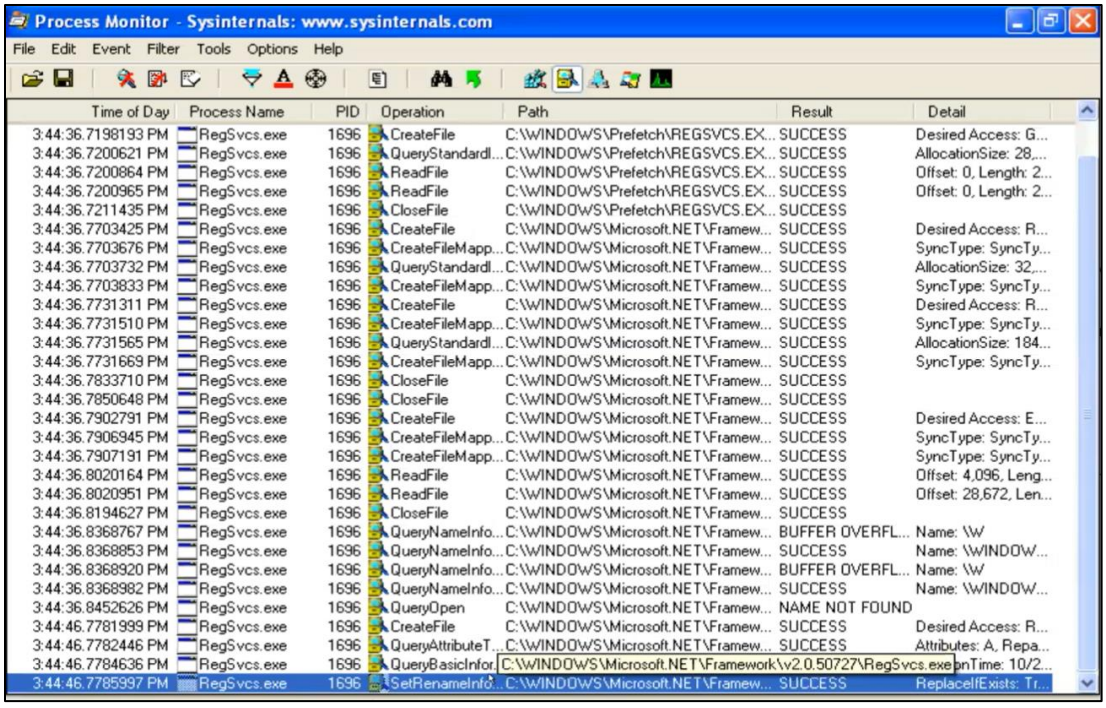
d. *GetKeyboardState* was found at 7E42D226. It retrieves the status of the specified virtual key.

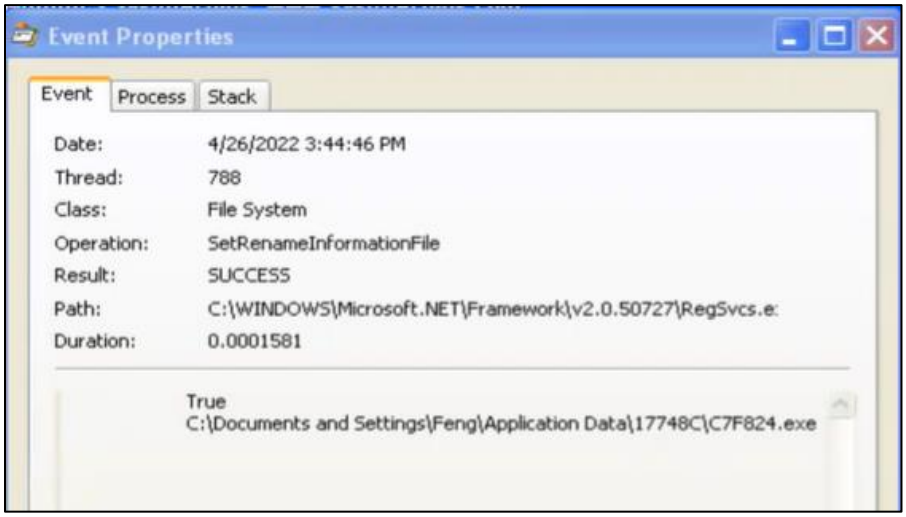
6. Analysis of 2nd RegSvcs.exe

The command line it uses for its creation is different from the 1st RegSvcs.exe. Below is the screenshot of the difference- This PID of the process in this run is 1296. It uses the same command line as the 2nd mur.exe

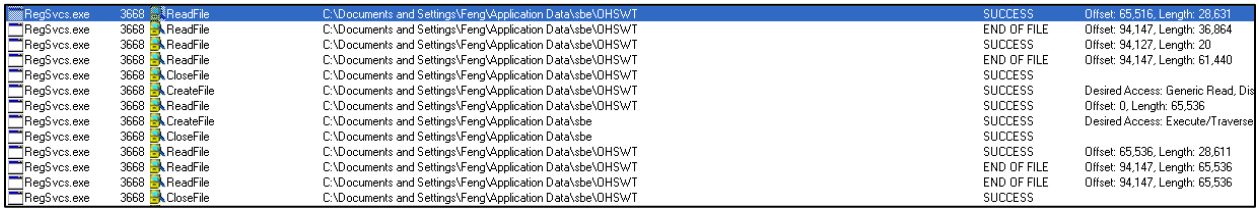


Loading its PID in the ProcessMonitor, it is observed that, the Regsvcs.exe was replaced with the filename as in the below screenshot and possibly deleted later for which there is no substantial evidence found. For this reason, if we try to look up for the exe in the directory, it cannot be located.





- The process is reading multiple offsets of the temporary file that was generated by 2nd mur.exe



- It creates a file named spd and deletes it later.

RegSvcs.exe	3668	CreateFile	C:\Documents and Settings\Feng\Application Data\sbe\spd	SUCCESS	Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Op
RegSvcs.exe	3668	QueryAttributeTagFile	C:\Documents and Settings\Feng\Application Data\sbe\spd	SUCCESS	Attributes: A, ReparseTag: 0x0
RegSvcs.exe	3668	SetDispositionInformationFile	C:\Documents and Settings\Feng\Application Data\sbe\spd	SUCCESS	Delete: True
RegSvcs.exe	3668	CloseFile	C:\Documents and Settings\Feng\Application Data\sbe\spd	SUCCESS	
RegSvcs.exe	3668	QueryDirectory	C:\Documents and Settings\Feng\Application Data\sbe	NO MORE FILES	
RegSvcs.exe	3668	CloseFile	C:\Documents and Settings\Feng\Application Data\sbe	SUCCESS	
RegSvcs.exe	3668	CreateFile	C:\Documents and Settings\Feng\Application Data\sbe\oio.ppt	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non

- It is observed that this process queries multiple registry keys. Once such interesting finding is shown below-

RegSvcs.exe	3668	RegCreateKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Desired Access: Write
RegSvcs.exe	3668	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WindowsUpdate	SUCCESS	Type: REG_SZ, Length: 196, Data: C:\Documents and Settings\Feng\Application Data\sbe\mur.exe C:\DOCUME~1\Feng\APPLIC~1\sbe\eam-wna
RegSvcs.exe	3668	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	SUCCESS	

→A registry key is created HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

This key contains commands that will be run each time a user logs on. (not at boot time)

→Then a value to the key is set under the name of WindowsUpdate. The value that is set is the command line used to execute the 1st mur.exe.

→ Lastly the registry is closed with all SUCCESS values which means this registry key is successfully created and its value is set.

From the above activity, we can therefore conclude that every time the user logs in the machine, mur.exe eam-wna malware is automatically run at the start time.

So, possibly the purpose of 2nd RegSvcs.exe is to make sure that the malware does not leave the user machine and make it difficult to find this malicious registry key as it is set under a genuine WindowsUpdate name.