

HW4

HW-B-1.exe

(Hint: printf() is 0x401089, main() is 0x401060)

1. Focus on the main() method. What is stored in EAX prior to the function call at 0x40107D?

.text:00401060 var_4	= byte ptr -4
.text:00401060 arg_0	= dword ptr 8
.text:00401060 arg_4	= dword ptr 0Ch
.text:00401060	
.text:00401060	push ebp
.text:00401061	mov ebp, esp
.text:00401063	push ecx
.text:00401064	mov [ebp+var_4], 0
.text:00401068	cmp [ebp+arg_0], 1
.text:0040106C	jle short loc_401085
.text:0040106E	mov eax, [ebp+arg_4]
.text:00401071	mov ecx, [eax+4]
.text:00401074	mov dl, [ecx]
.text:00401076	mov [ebp+var_4], dl
.text:00401079	mov al, [ebp+var_4]
.text:0040107C	push eax

the arg_4 value is inside eax prior to function call.

2. Focus on the function that starts at 0x401000. What does 0x62, 0x63, 0x73 likely correspond to?

0x62 likely coorespond to 'b'

0x63 likely coorespond to 'c'

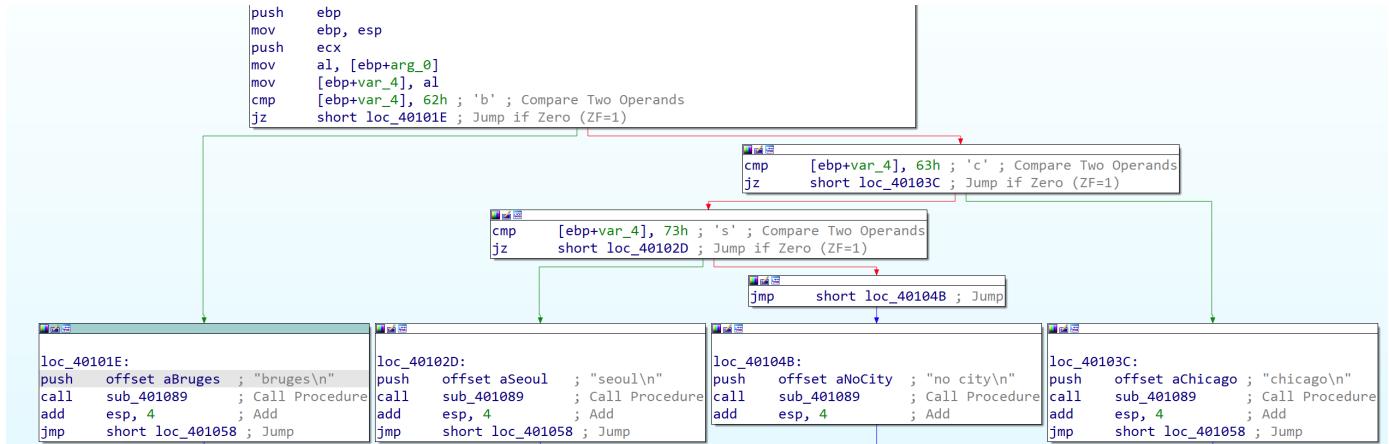
0x73 likely coorespond to 's'

```

.text:00401000 var_4          = byte ptr -4
.text:00401000 arg_0          = byte ptr 8
.text:00401000
.text:00401000                 push    ebp
.text:00401001                 mov     ebp, esp
.text:00401003                 push    ecx
.text:00401004                 mov     al, [ebp+arg_0]
.text:00401005                 mov     [ebp+var_4], al
.text:00401006                 cmp     [ebp+var_4], 62h ; 'b' ; Compare Two Operands
.text:00401007                 jz      short loc_40101E ; Jump if Zero (ZF=1)
.text:00401008                 cmp     [ebp+var_4], 63h ; 'c' ; Compare Two Operands
.text:00401009                 jz      short loc_40103C ; Jump if Zero (ZF=1)
.text:00401010                 cmp     [ebp+var_4], 73h ; 's' ; Compare Two Operands
.text:00401011                 jz      short loc_40102D ; Jump if Zero (ZF=1)
.text:00401012                 jmp     short loc_40104B ; Jump

```

The function compares the value stored inside var_4 to 98, 99, and 115 respectively and jumps to the correct timezone.



Implicitly this could be what it means:

b = bruges

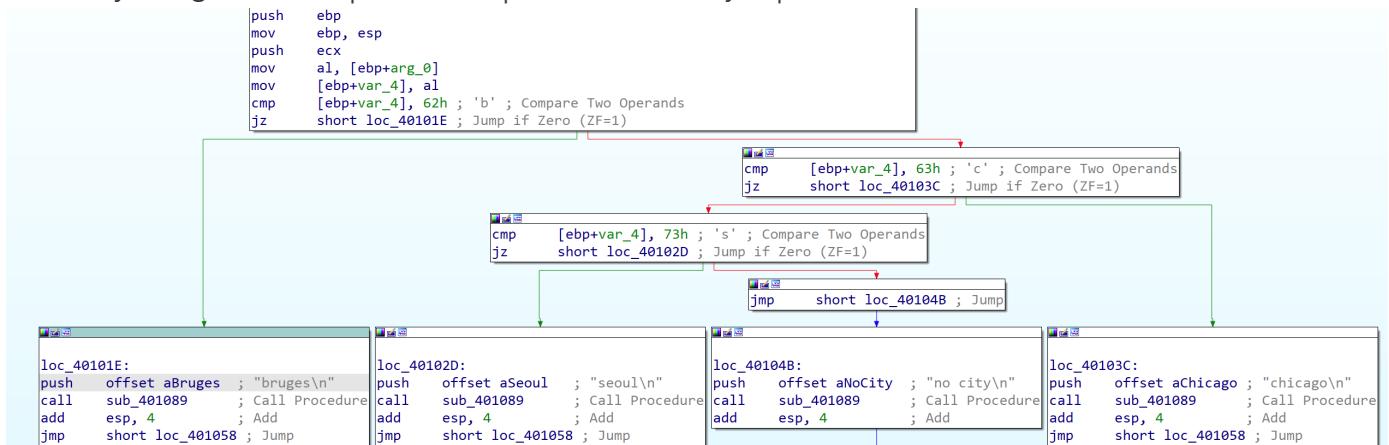
s = seoul

c = chicago

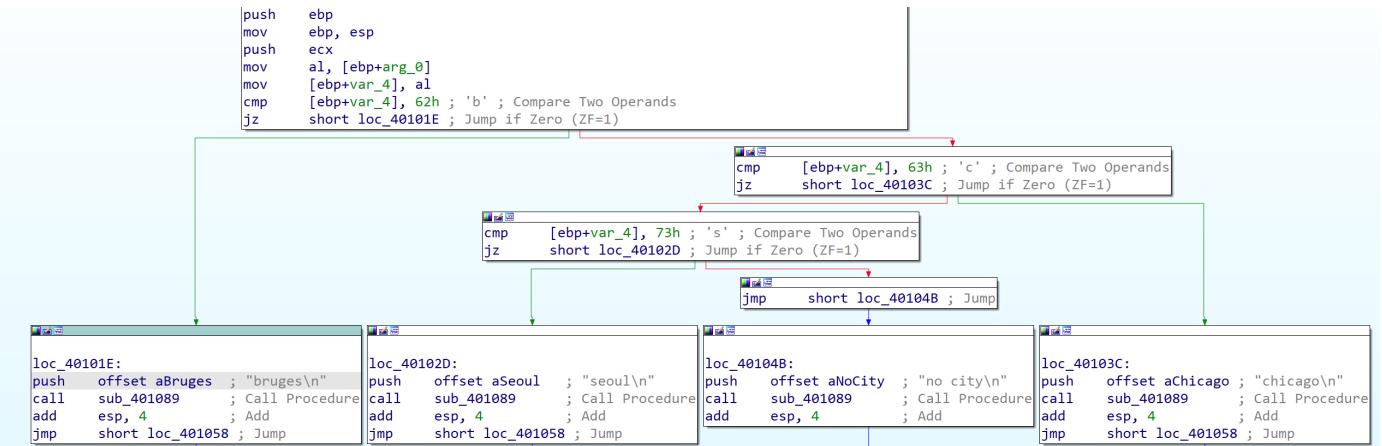
if none of the above, it would set a timezone.

3. What coding construct is likely a major part of this function?

It is likely using a switch operation implemented via a jump table.



4. What does this function (0x401000) do?



This function set the malware to the correct timezone.

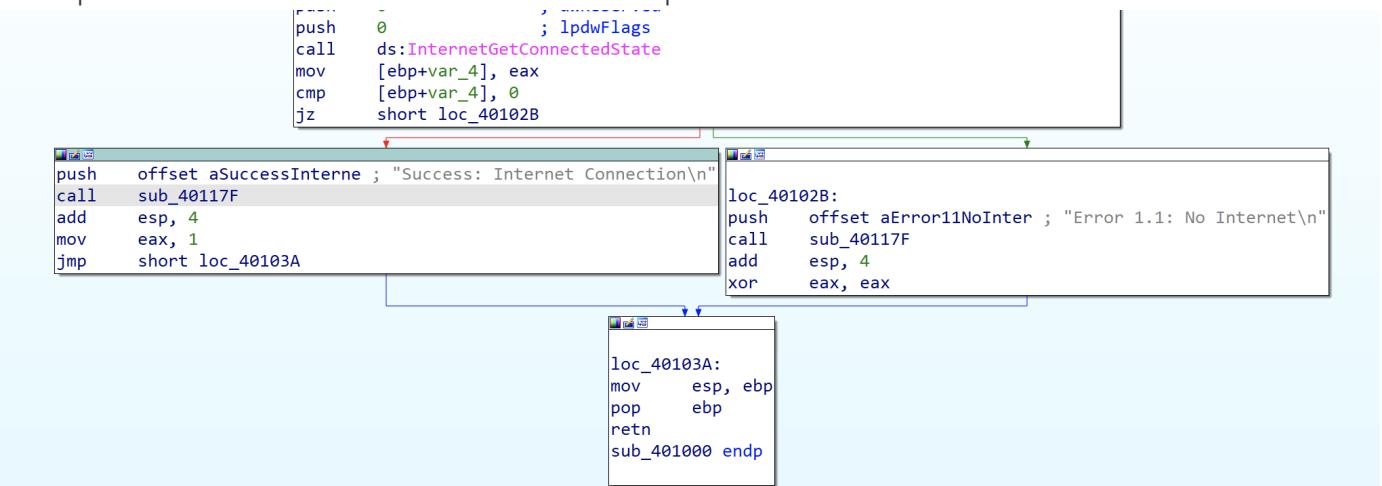
5. What does this overall program do?

The function finds the current time of the computer running the malware. If there is no time available, it inserts a timezone for it.

HW-B-3.exe

1. What is the subroutine located at 0x40117F?

It is a printf subroutine to inform whether the computer has internet connection or not.



It is a subroutine that is called after the malware checks whether the computer has internet connection.

2. What does the second subroutine called by main do?

```
.text:004011B0          public start
.text:004011B0  start      proc near
.text:004011B0
.text:004011B0  uExitCode    = dword ptr -20h
.text:004011B0  var_1C       = dword ptr -1Ch
.text:004011B0  ms_exc       = CPPEH_RECORD ptr -18h
.text:004011B0
.text:004011B0          push   ebp
.text:004011B1          mov    ebp, esp
.text:004011B3          push   0FFFFFFFh
.text:004011B5          push   offset stru_4060D0
.text:004011BA          push   offset sub_4027F8
.text:004011BF          mov    eax, large fs:0
.text:004011C5          push   eax
.text:004011C6          mov    large fs:0, esp
.text:004011CD          sub    esp, 10h
.text:004011D0          push   ebx
.text:004011D1          push   esi
.text:004011D2          push   edi
.text:004011D3          mov    [ebp+ms_exc.old_esp], esp
.text:004011D6          call   ds:GetVersion
.text:004011DC          xor    edx, edx
.text:004011DE          mov    dl, ah
.text:004011E0          mov    dword_409A08, edx
.text:004011E6          mov    ecx, eax
.text:004011E8          and    ecx, 0FFh
.text:004011EE          mov    dword_409A04, ecx
.text:004011F4          shl    ecx, 8
.text:004011F7          add    ecx, edx
.text:004011F9          mov    dword_409A00, ecx
.text:004011FF          shr    eax, 10h
.text:00401202          mov    dword_4099FC, eax
.text:00401207          push   0
.text:00401209          call   sub_4026A0
.text:0040120E          pop    ecx
```

the second subroutine called by main is sub_4026A0

```

.text:004026A0 ; ===== S U B R O U T I N E =====
.text:004026A0
.text:004026A0
.text:004026A0 sub_4026A0      proc near                  ; CODE XREF: start+59↑p
.text:004026A0
.text:004026A0     arg_0          = dword ptr  4
.text:004026A0
.text:004026A0     xor    eax, eax
.text:004026A2     push   0           ; dwMaximumSize
.text:004026A4     cmp    [esp+4+arg_0], eax
.text:004026A8     push   1000h       ; dwInitialSize
.text:004026AD     setz   al
.text:004026B0     push   eax          ; flOptions
.text:004026B1     call   ds:HeapCreate
.text:004026B7     test   eax, eax
.text:004026B9     mov    hHeap, eax
.text:004026BE     jz    short loc_4026F6
.text:004026C0     call   sub_402558
.text:004026C5     cmp    eax, 3
.text:004026C8     mov    dword_409DCC, eax
.text:004026CD     jnz   short loc_4026DC
.text:004026CF     push   3F8h
.text:004026D4     call   sub_403C9F
.text:004026D9     pop    ecx
.text:004026DA     jmp    short loc_4026E6
.text:004026DC ; -----

```

It allocates an executable private heap for the malware to run code which is probably stored in the .rsrc section.

3. What type of code construct is used in this subroutine?

If statement type code construct is used in this subroutine.

```

|.text:00401051      push   offset szAgent ; "Internet Explorer 7.5/pma"
|.text:00401056      call   ds:InternetOpenA
|.text:0040105C      mov    [ebp+hInternet], eax
|.text:0040105F      push   0           ; dwContext
|.text:00401061      push   0           ; dwFlags
|.text:00401063      push   0           ; dwHeadersLength
|.text:00401065      push   0           ; lpszHeaders
|.text:00401067      push   offset szUrl  ; "http://www.practicalmalwareanalysis.com"...
|.text:0040106C      mov    eax, [ebp+hInternet]
|.text:0040106F      push   eax          ; hInternet
|.text:00401070      call   ds:InternetOpenUrlA
|.text:00401076      mov    [ebp+hFile], eax
|.text:00401079      cmp    [ebp+hFile], 0
|.text:0040107D      jnz   short loc_40109D
|.text:0040107F      push   offset aError21FailToO ; "Error 2.1: Fail to OpenUrl\n"
|.text:00401084      call   sub_40117F
|.text:00401089      add    esp, 4
|.text:0040108C      mov    ecx, [ebp+hInternet]
|.text:0040108F      push   ecx          ; hInternet
|.text:00401090      call   ds:InternetCloseHandle
|.text:00401096      xor    al, al
|.text:00401098      jmp    loc_40112C
+-----.text:00401098 .

```

4. Are there any network-based indicators for this program?

Yes

1. It uses the WININET.dll which is for connecting to the internet

00000000004060B4	InternetOpenUrlA	WININET
00000000004060B8	InternetCloseHandle	WININET
00000000004060BC	InternetReadFile	WININET
00000000004060C0	InternetGetConnectedState	WININET
00000000004060C4	InternetOpenA	WININET

2. Analyzing with strings

.data:004070C4 0000002F C http://www.practicalmalwareanalysis.com/cc.htm
.data:004070F4 0000001A C Internet Explorer 7.5/pma
.data:00407110 0000001F C Success: Parsed command is %c\n
.data:004070C4 ; CHAR szUrl[]
·.data:004070C4 szUrl db 'http://www.practicalmalwareanalysis.com/cc.htm',0 ; DATA XREF: sub_401040+27↑o
·.data:004070C4 align 4

We see that it tries to connect to the website www.practicalmalwareanalysis.com/cc.htm

5. What is the purpose of this malware?

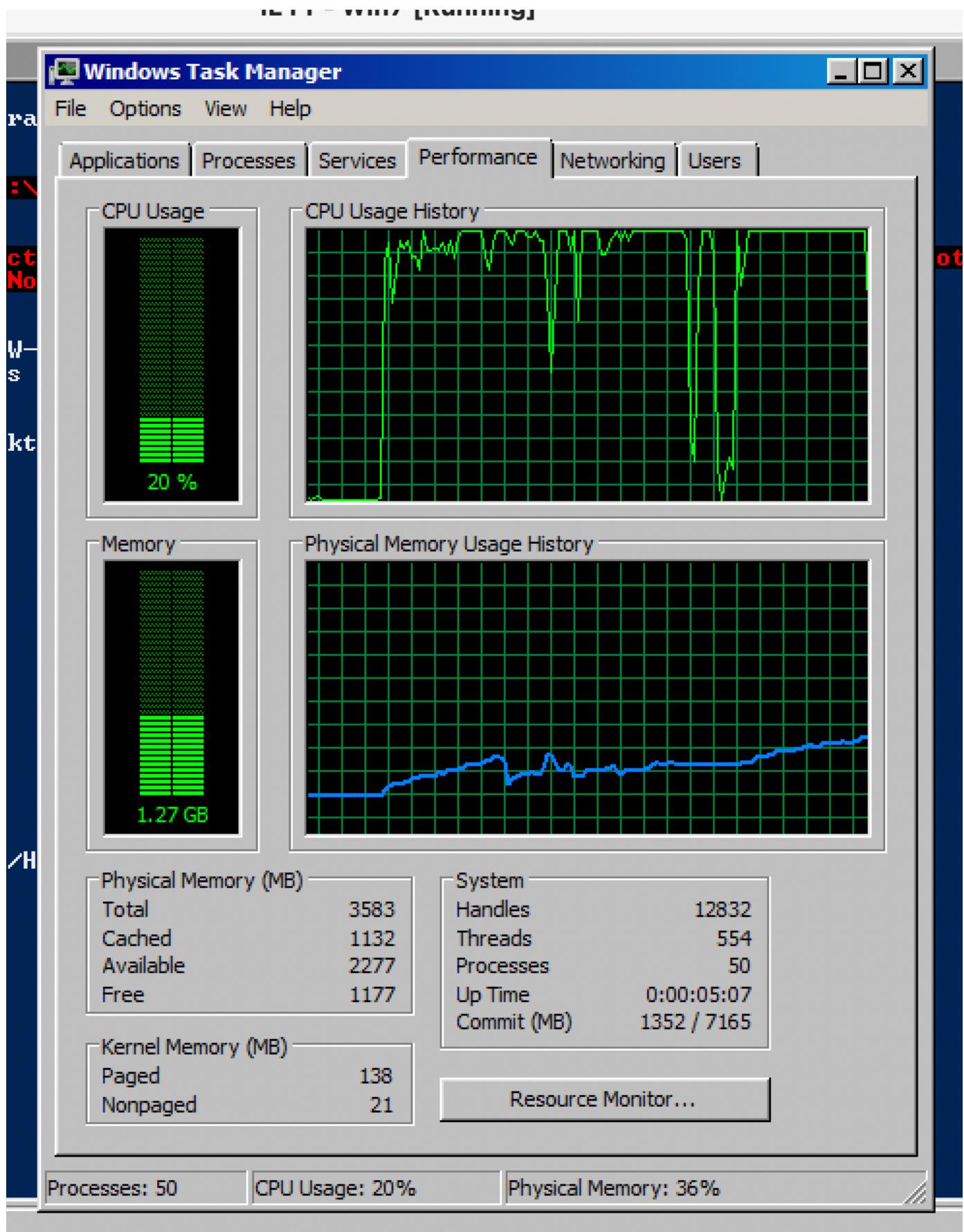
The purpose of this malware is to establish internet connection, open a malicious file, run malicious binary code on infected computer, then send the message to the attacker if the attack was a success.

.rdata:004068E8 00000014 C MultiByteToWideChar
.rdata:004068FE 0000000D C LCMMapStringA
.rdata:0040690E 0000000D C LCMMapStringW
.rdata:0040691E 0000000F C GetStringTypeA
.rdata:00406930 0000000F C GetStringTypeW
.rdata:00406942 0000000D C SetStdHandle
.rdata:00406952 0000000C C CloseHandle
.data:00407030 00000018 C Error 1.1: No Internet\n
.data:00407048 0000001E C Success: Internet Connection\n
.data:00407068 00000020 C Error 2.3: Fail to get command\n
.data:00407088 0000001D C Error 2.2: Fail to ReadFile\n
.data:004070A8 0000001C C Error 2.1: Fail to OpenUrl\n
.data:004070C4 0000002F C http://www.practicalmalwareanalysis.com/cc.htm
.data:004070F4 0000001A C Internet Explorer 7.5/pma
.data:00407110 0000001F C Success: Parsed command is %c\n

HW-B-8a.exe & HW-B-8b.dll

1. Run HW-B-8a.exe from the command line. What happens?

After:



The CPU usage increased from 500MB to 1.27GB.

Windows Task Manager

File Options View Help

Applications Processes Services Performance Networking Users

Name	PID	Description	Status	Group
VaultSvc		Credential ...	Stopped	
SamSs	472	Security Ac...	Running	
ProtectedSt...		Protected S...	Stopped	
NetTcpPort...		Net.Tcp Po...	Stopped	
NetTcpActiv...		Net.Tcp Lis...	Stopped	
NetPipeActiv...		Net.Pipe Lis...	Stopped	
NetMsmqAc...		Net.Msmq L...	Stopped	
Netlogon		Netlogon	Stopped	
KeyIso		CNG Key Is...	Stopped	
idsvc		Windows C...	Stopped	
EFS		Encrypting ...	Stopped	
AxInstSV		ActiveX Ins...	Stopped	AxInstSVGr...
bthserv		Bluetooth S...	Stopped	bthsrvcs
Power	588	Power	Running	DcomLaunch
PlugPlay	588	Plug and Play	Running	DcomLaunch
DcomLaunch	588	DCOM Serv...	Running	DcomLaunch
WinHttpAut...	872	WinHTTP W...	Running	LocalService
WebClient		WebClient	Stopped	LocalService
WdiService...	872	Diagnostic ...	Running	LocalService
W32Time		Windows Time	Stopped	LocalService
THREADOR...		Thread Ord...	Stopped	LocalService
SstpSvc		Secure Soc...	Stopped	LocalService
sppuินotify		SPP Notific...	Stopped	LocalService
nsi	872	Network St...	Running	LocalService
netprofm	872	Network Lis...	Running	LocalService

Services...

Processes: 49 CPU Usage: 100% Physical Memory: 34%

Graphically nothing changes on the interface

```
PS C:\Users\IEUser\Desktop\HW-B> ./HW-B-8a.exe
PS C:\Users\IEUser\Desktop\HW-B> ./HW-B-8a.exe
PS C:\Users\IEUser\Desktop\HW-B> ls
```

Internally, the following files are modified.

Select Administrator: Windows PowerShell			
d----	7/13/2009	7:05 PM	SchCache
d----	7/13/2009	9:52 PM	schemas
d----	7/14/2009	12:22 AM	security
d----	7/13/2009	9:34 PM	ServiceProfiles
d----	1/2/2018	6:43 PM	servicing
d----	7/13/2009	9:34 PM	Setup
d----	1/2/2018	9:03 PM	SoftwareDistribution
d----	7/13/2009	9:56 PM	Speech
d----	7/13/2009	9:52 PM	system
i----	11/14/2021	7:39 PM	System32
d----	7/13/2009	9:46 PM	TAPI
d----	7/13/2009	9:53 PM	Tasks
d----	11/14/2021	7:42 PM	Temp
d----	1/2/2018	8:44 PM	tracing
d----	7/13/2009	9:52 PM	twain_32
d----	7/13/2009	2:37 PM	Uss
d----	7/13/2009	9:52 PM	Web
d----	11/14/2021	7:29 PM	winsxs
-a---	11/20/2010	4:16 AM	65024 bfsvc.exe
-a-s	11/14/2021	7:29 PM	67584 bootstat.dat
-a---	1/2/2018	5:20 PM	1774 DtcInstall.log
-a---	6/10/2009	2:14 PM	53555 Enterprise.xml
-a---	8/29/2016	7:55 AM	2972672 explorer.exe
-a---	7/13/2009	6:14 PM	13824 fveupdate.exe
-a---	6/2/2017	12:57 AM	497152 HelpPane.exe
-a---	7/13/2009	6:14 PM	15360 hh.exe
-a---	1/2/2018	7:24 PM	13089 IE11_main.log
-a---	7/13/2009	3:58 PM	43131 mib.bin
-a---	6/10/2009	2:19 PM	1405 msdfmap.ini
-a---	7/9/2015	10:42 AM	179712 notepad.exe
-a---	1/2/2018	8:08 PM	16240 PFRO.log
-a---	7/13/2009	6:14 PM	398336 regedit.exe
-a---	11/14/2021	7:29 PM	16025 setupact.log
-a---	7/13/2009	9:39 PM	0 setuperr.log
-a---	6/10/2009	2:14 PM	48201 Starter.xml
-a---	6/10/2009	2:46 PM	219 system.ini
-a---	1/2/2018	5:20 PM	1313 TSSysprep.log
-a---	6/10/2009	2:41 PM	94784 twain.dll
-a---	11/20/2010	4:21 AM	51200 twain_32.dll
-a---	6/10/2009	2:41 PM	49680 twunk_16.exe
-a---	7/13/2009	6:14 PM	31232 twunk_32.exe
-a---	7/13/2009	9:54 PM	403 win.ini
-a---	11/14/2021	7:40 PM	1189489 WindowsUpdate.log
-a---	6/10/2009	2:42 PM	256192 winhelp.exe
-a---	7/13/2009	6:14 PM	9728 winhlp32.exe
-a---	6/10/2009	2:34 PM	316640 WMSysPr9.prx
-a---	7/13/2009	6:14 PM	9216 write.exe
-a---	6/10/2009	2:42 PM	707 _default.pif



7:45 PM
11/14/2021

Select Administrator: Windows PowerShell

d----	7/13/2009	7:05 PM	SchCache
d----	7/13/2009	9:52 PM	schemas
d----	7/14/2009	12:22 AM	security
d----	7/13/2009	9:34 PM	ServiceProfiles
d----	1/2/2018	6:43 PM	servicing
d----	7/13/2009	9:34 PM	Setup
d----	1/2/2018	9:03 PM	SoftwareDistribution
d----	7/13/2009	9:56 PM	Speech
d----	7/13/2009	9:52 PM	system
d----	11/14/2021	7:39 PM	System32
d----	7/13/2009	9:46 PM	TAPI
d----	7/13/2009	9:53 PM	Tasks
d----	11/14/2021	7:42 PM	Temp
d----	1/2/2018	8:44 PM	tracing
d----	7/13/2009	9:52 PM	twain_32
d----	7/13/2009	7:37 PM	Vss
d----	7/13/2009	9:52 PM	Web
d----	11/14/2021	7:29 PM	winsxs
-a---	11/20/2010	4:16 AM	65024 hfsvc.exe
-a--s	11/14/2021	7:29 PM	67584 bootstat.dat
-a---	1/2/2018	5:20 PM	1774 DtcInstall.log
-a---	6/10/2009	2:14 PM	53555 Enterprise.xml
-a---	8/29/2016	7:55 AM	2972672 explorer.exe
-a---	7/13/2009	6:14 PM	13824 fveupdate.exe
-a---	6/2/2017	12:57 AM	497152 HelpPane.exe
-a---	7/13/2009	6:14 PM	15360 hh.exe
-a---	1/2/2018	7:24 PM	13089 IE11_main.log
-a---	7/13/2009	3:58 PM	43131 mib.bin
-a---	6/10/2009	2:19 PM	1405 msdfmap.ini
-a---	7/9/2015	10:42 AM	179712 notepad.exe
-a---	1/2/2018	8:08 PM	16240 PFR0.log
-a---	7/13/2009	6:14 PM	398336 regedit.exe
-a---	11/14/2021	7:29 PM	16025 setupact.log
-a---	7/13/2009	9:39 PM	0 setuperr.log
-a---	6/10/2009	2:14 PM	48201 Starter.xml
-a---	6/10/2009	2:46 PM	219 system.ini
-a---	1/2/2018	5:20 PM	1313 TSSysprep.log
-a---	6/10/2009	2:41 PM	94784 twain.dll
-a---	11/20/2010	4:21 AM	51200 twain_32.dll
-a---	6/10/2009	2:41 PM	49680 twunk_16.exe
-a---	7/13/2009	6:14 PM	31232 twunk_32.exe
-a---	7/13/2009	9:54 PM	403 win.ini
-a---	11/14/2021	7:40 PM	1189489 WindowsUpdate.log
-a---	6/10/2009	2:42 PM	256192 winhelp.exe
-a---	7/13/2009	6:14 PM	9728 winhlp32.exe
-a---	6/10/2009	2:34 PM	316640 WMSysPr9.prx
-a---	7/13/2009	6:14 PM	9216 write.exe
-a---	6/10/2009	2:42 PM	707 _default.pif

Select Administrator: Windows PowerShell

d----	7/13/2009	7:05 PM	SchCache
d----	7/13/2009	9:52 PM	schemas
d----	7/14/2009	12:22 AM	security
d----	7/13/2009	9:34 PM	ServiceProfiles
d----	1/2/2018	6:43 PM	servicing
d----	7/13/2009	9:34 PM	Setup
d----	1/2/2018	9:03 PM	SoftwareDistribution
d----	7/13/2009	9:56 PM	Speech
d----	7/13/2009	9:52 PM	system
d----	11/14/2021	7:39 PM	System32
d----	7/13/2009	9:46 PM	IAPI
d----	7/13/2009	9:53 PM	Tasks
d----	11/14/2021	7:42 PM	Temp
d----	1/2/2018	8:44 PM	tracing
d----	7/13/2009	9:52 PM	twain_32
d----	7/13/2009	7:37 PM	Uss
d----	7/13/2009	9:52 PM	Web
d----	11/14/2021	7:29 PM	winsxs
-a---	11/20/2010	4:16 AM	65024 bfcsvc.exe
-a--s	11/14/2021	7:29 PM	67584 bootstat.dat
-a---	1/2/2018	5:20 PM	1774 DtcInstall.log
-a---	6/10/2009	2:14 PM	53555 Enterprise.xml
-a---	8/29/2016	7:55 AM	2972672 explorer.exe
-a---	7/13/2009	6:14 PM	13824 fveupdate.exe
-a---	6/2/2017	12:57 AM	497152 HelpPane.exe
-a---	7/13/2009	6:14 PM	15360 hh.exe
-a---	1/2/2018	7:24 PM	13089 IE11_main.log
-a---	7/13/2009	3:58 PM	43131 mib.bin
-a---	6/10/2009	2:19 PM	1405 msdfmap.ini
-a---	7/9/2015	10:42 AM	179712 notepad.exe
-a---	1/2/2018	8:08 PM	16240 PFRO.log
-a---	7/13/2009	6:14 PM	398336 regedit.exe
-a---	11/14/2021	7:29 PM	16025 setupact.log
-a---	7/13/2009	9:39 PM	0 setuperr.log
-a---	6/10/2009	2:14 PM	48201 Starter.xml
-a---	6/10/2009	2:46 PM	219 system.ini
-a---	1/2/2018	5:20 PM	1313 TSSysprep.log
-a---	6/10/2009	2:41 PM	94784 twain.dll
-a---	11/20/2010	4:21 AM	51200 twain_32.dll
-a---	6/10/2009	2:41 PM	49680 twunk_16.exe
-a---	7/13/2009	6:14 PM	31232 twunk_32.exe
-a---	7/13/2009	9:54 PM	403 win.ini
-a---	11/14/2021	7:40 PM	1189489 WindowsUpdate.log
-a---	6/10/2009	2:42 PM	256192 winhelp.exe
-a---	7/13/2009	6:14 PM	9728 winhlp32.exe
-a---	6/10/2009	2:34 PM	316640 WMSysPr9.prx
-a---	7/13/2009	6:14 PM	9216 write.exe
-a---	6/10/2009	2:42 PM	707 _default.pif

Select Administrator: Windows PowerShell

d----	7/13/2009	7:05 PM	SchCache
d----	7/13/2009	9:52 PM	schemas
d----	7/14/2009	12:22 AM	security
d----	7/13/2009	9:34 PM	ServiceProfiles
d----	1/2/2018	6:43 PM	servicing
d----	7/13/2009	9:34 PM	Setup
d----	1/2/2018	9:03 PM	SoftwareDistribution
d----	7/13/2009	9:56 PM	Speech
d----	7/13/2009	9:52 PM	system
d----	11/14/2021	7:39 PM	System32
d----	7/13/2009	9:46 PM	TAPI
d----	7/13/2009	9:53 PM	Tasks
d----	11/14/2021	7:42 PM	Temp
d----	1/2/2018	8:44 PM	tracing
d----	7/13/2009	9:52 PM	twain_32
d----	7/13/2009	7:37 PM	Uss
d----	7/13/2009	9:52 PM	Web
d----	11/14/2021	7:29 PM	winsxs
-a---	11/20/2010	4:16 AM	65024 bfcsvc.exe
-a--s	11/14/2021	7:29 PM	67584 bootstat.dat
-a---	1/2/2018	5:20 PM	1774 DtcInstall.log
-a---	6/10/2009	2:14 PM	53555 Enterprise.xml
-a---	8/29/2016	7:55 AM	2972672 explorer.exe
-a---	7/13/2009	6:14 PM	13824 fveupdate.exe
-a---	6/2/2017	12:57 AM	497152 HelpPane.exe
-a---	7/13/2009	6:14 PM	15360 hh.exe
-a---	1/2/2018	7:24 PM	13089 IE11_main.log
-a---	7/13/2009	3:58 PM	43131 mib.bin
-a---	6/10/2009	2:19 PM	1405 msdfmap.ini
-a---	7/9/2015	10:42 AM	179712 notepad.exe
-a---	1/2/2018	8:08 PM	16240 PFRO.log
-a---	7/13/2009	6:14 PM	398336 regedit.exe
-a---	11/14/2021	7:29 PM	16025 setupact.log
-a---	7/13/2009	9:39 PM	0 setuperr.log
-a---	6/10/2009	2:14 PM	48201 Starter.xml
-a---	6/10/2009	2:46 PM	219 system.ini
-a---	1/2/2018	5:20 PM	1313 TSSysprep.log
-a---	6/10/2009	2:41 PM	94784 twain.dll
-a---	11/20/2010	4:21 AM	51200 twain_32.dll
-a---	6/10/2009	2:41 PM	49680 twunk_16.exe
-a---	7/13/2009	6:14 PM	31232 twunk_32.exe
-a---	7/13/2009	9:54 PM	403 win.ini
-a---	11/14/2021	7:40 PM	1189489 WindowsUpdate.log
-a---	6/10/2009	2:42 PM	256192 winhelp.exe
-a---	7/13/2009	6:14 PM	9728 winhlp32.exe
-a---	6/10/2009	2:34 PM	316640 WMSysPr9.prx
-a---	7/13/2009	6:14 PM	9216 write.exe
-a---	6/10/2009	2:42 PM	707 _default.pif

Select Administrator: Windows PowerShell

d----	7/13/2009	9:34 PM		ServiceProfiles
d----	1/2/2018	6:43 PM		servicing
d----	7/13/2009	9:34 PM		Setup
d----	1/2/2018	9:03 PM		SoftwareDistribution
d----	7/13/2009	9:56 PM		Speech
d----	7/13/2009	9:52 PM		system
d----	11/14/2021	7:39 PM		System32
d----	7/13/2009	9:46 PM		TAPI
d----	7/13/2009	9:53 PM		Tasks
d----	11/14/2021	7:42 PM		Temp
d----	1/2/2018	8:44 PM		tracing
d----	7/13/2009	9:52 PM		twain_32
d----	7/13/2009	7:37 PM		Uss
d----	7/13/2009	9:52 PM		Web
d----	11/14/2021	7:29 PM		winsxs
-a---	11/20/2010	4:16 AM	65024	bfsvc.exe
-a--s	11/14/2021	7:29 PM	67584	bootstat.dat
-a---	1/2/2018	5:20 PM	1774	DtcInstall.log
-a---	6/10/2009	2:14 PM	53555	Enterprise.xml
-a---	8/29/2016	7:55 AM	2972672	explorer.exe
-a---	7/13/2009	6:14 PM	13824	fveupdate.exe
-a---	6/2/2017	12:57 AM	497152	HelpPane.exe
-a---	7/13/2009	6:14 PM	15360	hh.exe
-a---	1/2/2018	7:24 PM	13089	IE11_main.log
-a---	7/13/2009	3:58 PM	43131	mib.bin
-a---	6/10/2009	2:19 PM	1405	msdfmap.ini
-a---	7/9/2015	10:42 AM	179712	notepad.exe
-a---	1/2/2018	8:08 PM	16240	PFR0.log
-a---	7/13/2009	6:14 PM	398336	regedit.exe
-a---	11/14/2021	7:29 PM	16025	setupact.log
-a---	7/13/2009	9:39 PM	0	setuperr.log
-a---	6/10/2009	2:14 PM	48201	Starter.xml
-a---	6/10/2009	2:46 PM	219	system.ini
-a---	1/2/2018	5:20 PM	1313	TSSysprep.log
-a---	6/10/2009	2:41 PM	94784	twain.dll
-a---	11/20/2010	4:21 AM	51200	twain_32.dll
-a---	6/10/2009	2:41 PM	49680	twunk_16.exe
-a---	7/13/2009	6:14 PM	31232	twunk_32.exe
-a---	7/13/2009	9:54 PM	403	win.ini
-a---	11/14/2021	7:40 PM	1189489	WindowsUpdate.log
-a---	6/10/2009	2:42 PM	256192	winhelp.exe
-a---	7/13/2009	6:14 PM	9728	winhlp32.exe
-a---	6/10/2009	2:34 PM	316640	WMSysPr9.prx
-a---	7/13/2009	6:14 PM	9216	write.exe
-a---	6/10/2009	2:42 PM	707	_default.pif

2. What method does HW-B-8a.exe use to perform covert launching?

It uses a DLL injection. DLL injection is a form of process injection where a remote process is forced to load a malicious DLL.

1. Injecting code into a remote process

1. LoadLibrary

The screenshot shows the Immunity Debugger's Imports window. The table lists 15 entries from the KERNEL32 library. The columns are Address, Ordinal, Name, and Library. The 'Name' column contains function names like TlsGetValue, TlsSetValue, TlsFree, EnterCriticalSection, LeaveCriticalSection, HeapFree, Sleep, WideCharToMultiByte, GetStringTypeW, LCMapStringW, LoadLibraryExW, OutputDebugStringW, LoadLibraryW, and RtlUnwind. The 'Library' column shows all entries are from KERNEL32. The row for LoadLibraryW is highlighted with a blue selection bar.

Address	Ordinal	Name	Library
004080C0		TlsGetValue	KERNEL32
004080C4		TlsSetValue	KERNEL32
004080C8		TlsFree	KERNEL32
004080D0		EnterCriticalSection	KERNEL32
004080D4		LeaveCriticalSection	KERNEL32
004080D8		HeapFree	KERNEL32
004080E0		Sleep	KERNEL32
004080E4		WideCharToMultiByte	KERNEL32
004080E8		GetStringTypeW	KERNEL32
004080F0		LCMapStringW	KERNEL32
004080F4		LoadLibraryExW	KERNEL32
004080F8		OutputDebugStringW	KERNEL32
004080FC		LoadLibraryW	KERNEL32
004080F4		RtlUnwind	KERNEL32

2. obtain a handle to the victim process (search the process list for the injection target)
 1. **CreateToolhelp32Snapshot**
 2. **Process32First**
 3. **Process32Next**
3. launcher retrieves the process identifier (PID) of the target process and then uses it to obtain the handle
 1. **OpenProcess**

Address	Ordinal	Name	Library
00408000		GetSystemTimeAsFileTime	KERNEL32
00408004		WriteConsoleW	KERNEL32
00408008		SetFilePointerEx	KERNEL32
0040800C		SetStdHandle	KERNEL32
00408010		GetProcAddress	KERNEL32
00408014		VirtualAllocEx	KERNEL32
00408018		OpenProcess	KERNEL32
0040801C		CreateRemoteThread	KERNEL32
00408020		WriteProcessMemory	KERNEL32
00408024		CloseHandle	KERNEL32
00408028		lstrcatA	KERNEL32
0040802C		GetModuleHandleW	KERNEL32
00408030		GetCurrentDirectoryA	KERNEL32
00408034		GetCommandLineW	KERNEL32

4. launcher malware to create and execute a new thread in a remote process

1. CreateRemoteThread

1. 3 Parameters:

1. **hProcess**: process handle obtained
2. **OpenProcess**
3. **lpStartAddress** : starting point of the injected thread
4. **lpParameter**: an argument for that thread

Address	Ordinal	Name	Library
00408000		GetSystemTimeAsFileTime	KERNEL32
00408004		WriteConsoleW	KERNEL32
00408008		SetFilePointerEx	KERNEL32
0040800C		SetStdHandle	KERNEL32
00408010		GetProcAddress	KERNEL32
00408014		VirtualAllocEx	KERNEL32
00408018		OpenProcess	KERNEL32
0040801C		CreateRemoteThread	KERNEL32
00408020		WriteProcessMemory	KERNEL32
00408024		CloseHandle	KERNEL32
00408028		lstrcmpA	KERNEL32
0040802C		GetModuleHandleW	KERNEL32
00408030		GetCurrentDirectoryA	KERNEL32
00408034		GetCommandLineW	KERNEL32

5. create space for the malicious library name string

1. VirtualAllocEx

Address	Ordinal	Name	Library
00408004		WriteConsoleW	KERNEL32
00408008		SetFilePointerEx	KERNEL32
0040800C		SetStdHandle	KERNEL32
00408010		GetProcAddress	KERNEL32
00408014		VirtualAllocEx	KERNEL32
00408018		OpenProcess	KERNEL32
0040801C		CreateRemoteThread	KERNEL32
00408020		WriteProcessMemory	KERNEL32
00408024		CloseHandle	KERNEL32
00408028		lstrcmpA	KERNEL32
0040802C		GetModuleHandleW	KERNEL32
00408030		GetCurrentDirectoryA	KERNEL32
00408034		GetCommandLineW	KERNEL32
00408038		IsDebuggerPresent	KERNEL32

6. writes the malicious library name string into the memory space that was allocated with

VirtualAllocEx

1. CreateRemoteThread

2. WriteProcessMemory

Address	Ordinal	Name	Library
00408004		WriteConsoleW	KERNEL32
00408008		SetFilePointerEx	KERNEL32
0040800C		SetStdHandle	KERNEL32
00408010		GetProcAddress	KERNEL32
00408014		VirtualAllocEx	KERNEL32
00408018		OpenProcess	KERNEL32
0040801C		CreateRemoteThread	KERNEL32
00408020		WriteProcessMemory	KERNEL32
00408024		CloseHandle	KERNEL32
00408028		lstrcatA	KERNEL32
0040802C		GetModuleHandleW	KERNEL32
00408030		GetCurrentDirectoryA	KERNEL32
00408034		GetCommandLineW	KERNEL32
00408038		IsDebuggerPresent	KERNEL32

3. What process is targeted by the malware?

The wuauct.exe process is targeted by the malware

WindowsUpdate.log - Notepad					
File	Edit	Format	View	Help	
908	f60	Agent	*	{2A6BAB0A-1347-475B-A035-14C5E660A717}.200	
908	f60	DnldMgr	*****	DnldMgr: Regulation Refresh [svc: {7971F918-A847-4430	
908	f60	DnldMgr	*	Regulation call complete. 0x00000000	
908	f60	DnldMgr	*****	DnldMgr: New download job [updateId = {2A6BAB0A-1347-	
908	f60	DnldMgr	*	Queueing update for download handler request generation.	
908	f60	DnldMgr	Generating	download request for update {2A6BAB0A-1347-475B-A035-14	
908	f60	Handler	Generating	request for CBS update 2A6BAB0A-1347-475B-A035-14C5E660	
908	f60	Handler	Selected	payload type is pteExpress	
908	f60	Handler	UH:	DpxRestoreJob returned 0x80070002	
908	f60	Handler	Detected	download state is dsHavePackage	
908	3c0	AU	>>## RESUMED ## AU:	Download update [updateId = {3CC14D64-9917-4	
908	3c0	AU	# WARNING:	Download failed, error = 0x80092004	
908	3c0	AU	Successfully	wrote event for AU health state:0	
908	d90	AU	Launched	new AU client for directive 'Download Progress', session	
3160	450	Misc	=====	Logging initialized (build: 7.6.7601.23806, tz: -0800	
3160	450	Misc	= Process:	C:\windows\system32\wuauct.exe	
3160	450	AUClnt	Launched	Client UI process	
3160	450	Misc	=====	Logging initialized (build: 7.6.7601.23806, tz: -0800	
3160	450	Misc	= Process:	C:\windows\system32\wuauct.exe	
3160	450	Misc	= Module:	C:\Windows\system32\wucltux.dll	
3160	450	cltUI	AU client	got new directive = 'Download Progress', serviceId = {79	
908	e00	Handler	FATAL:	CBS called Error with 0x80092004,	
908	f60	Handler	FATAL:	UH: 0x80092004: Async stage operation failed in CUHCbsHandl	
908	f60	Handler	FATAL:	Request generation for CBS update complete with hr=0x800920	
908	f60	Handler	FATAL:	Error source is 106.	
908	f60	DnldMgr	FATAL:	DM:CAgentDownloadManager::GenerateAllDownloadRequests: Gene	
908	f60	DnldMgr	WARNING:	Download request generation failed with 0x80092004.	
908	f60	DnldMgr	Error	0x80092004 occurred while downloading update; notifying depe	

It also runs the MpCmdRun.exe

-a---	11/12/2020	11:45 PM	10771674	Microsoft .NET Frame si.txt
-a---	11/12/2020	11:46 PM	663410	Microsoft .NET Frame
-a---	11/15/2021	8:43 PM	1778	MpCmdRun.log
-a---	11/12/2020	11:56 PM	19624	MpSigStub.log
-a---	1/2/2018	9:01 PM	9781427	openssh.exe
-a---	1/2/2018	9:01 PM	145	PATH

SelfUpdate

Windows 7 (C:) Windows SoftwareDistribution SelfUpdate

Organize Include in library Share with New folder

Name	Date modified	Type	Size
Handler	1/2/2018 5:23 PM	File folder	
wsus3setup.cab	11/12/2020 11:40 PM	Cabinet File	33 KB
WUClient-SelfUpdate-ActiveX~31bf3856ad3...	6/2/2012 5:58 PM	MUM File	5 KB
WUClient-SelfUpdate-ActiveX~31bf3856ad3...	5/14/2014 11:52 AM	MUM File	5 KB
WUClient-SelfUpdate-Aux-TopLevel~31bf38...	6/2/2012 5:58 PM	MUM File	508 KB
WUClient-SelfUpdate-Aux-TopLevel~31bf38...	5/14/2014 11:52 AM	MUM File	508 KB
WUClient-SelfUpdate-Core-TopLevel~31bf3...	6/2/2012 5:58 PM	MUM File	832 KB
WUClient-SelfUpdate-Core-TopLevel~31bf3...	5/14/2014 11:52 AM	MUM File	832 KB
wuident.cab	11/15/2021 10:20 PM	Cabinet File	20 KB
wuident.txt	11/15/2021 10:20 PM	Text Document	4 KB
wuident-inner.cab	5/22/2014 5:07 PM	Cabinet File	12 KB
WuPackages.xml	5/14/2014 11:52 AM	XML Document	1 KB

12 items