

Volatility

ENG-USTXHOU-148 (jackr-challenge)

ImageInfo

```
$ python2.7 vol.py -f ~/Downloads/jackcr-  
challenge/ENG-USTXHOU-148/memdump.bin  
imageinfo
```

Suggested Profile(s) : **WinXPSP2x86**, WinXPSP3x86
(Instantiated with WinXPSP2x86)

KDBG : **0x8054cde0L**

Network Connections

```
$ python2.7 vol.py -f ~/Downloads/jackcr-  
challenge/ENG-USTXHOU-148/memdump.bin --  
profile=WinXPSP2x86 --kdbg=0x8054cde0  
connscan
```

Offset(P)	Local Address	Remote Address	Pid
0x01ffa850	172.16.150.20:1291	58.64.132.141:80	1024
0x189e8850	172.16.150.20:1291	58.64.132.141:80	1024

Whois

```
$ whois 58.64.132.141
```

inetnum:	58.64.132.0 - 58.64.132.255
netname:	NWTiDC-HK
descr:	NWT iDC Data Service
country:	HK

Processes

```
$ python2.7 vol.py -f ~/Downloads/jackcr-  
challenge/ENG-USTXHOU-148/memdump.bin --  
profile=WinXPSP2x86 --kdbg=0x8054cde0 pstree
```

Name	Pid	PPid	Thds	Hnds	Time
0x823c8830:System	4	0	51	271	1970-01-01 00:00:00 UTC+0000
. 0x821841c8:smss.exe	356	4	3	19	2012-11-26 22:03:28 UTC+0000
.. 0x82189da0:winlogon.exe	628	356	18	653	2012-11-26 22:03:29 UTC+0000
... 0x82194650:services.exe	680	628	15	243	2012-11-26 22:03:30 UTC+0000
.... 0x820b3da0:svchost.exe	1024	680	76	1645	2012-11-26 22:03:32 UTC+0000
..... 0x82045da0:wuaucit.exe	1628	1024	3	142	2012-11-26 22:04:43 UTC+0000
..... 0x82049690:wc.exe	364	1024	1	27	2012-11-27 01:30:00 UTC+0000

Consoles

```
$ python2.7 vol.py -f ~/Downloads/jackcr-challenge/ENG-USTXHOU-148/  
memdump.bin --profile=WinXPSP2x86 --kdbg=0x8054cde0 consoles
```

```
ConsoleProcess: csrss.exe Pid: 604  
Console: 0x4f3318 CommandHistorySize: 50  
HistoryBufferCount: 1 HistoryBufferMax: 4  
OriginalTitle: %SystemRoot%\System32\svchost.exe  
Title: C:\WINDOWS\System32\svchost.exe  
AttachedProcess: wc.exe Pid: 364 Handle: 0x424
```

```
CommandHistory: 0x4f4db0 Application: wc.exe Flags: Allocated  
CommandCount: 0 LastAdded: -1 LastDisplayed: -1  
FirstCommand: 0 CommandCountMax: 50  
ProcessHandle: 0x424
```

```
Screen 0x4f3a20 X:80 Y:25
```

```
Dump:
```

```
WCE v1.3beta (Windows Credentials Editor) - (c) 2010,2011,2012 Amplia Security -  
by Hernan Ochoa (hernan@ampliasecurity.com)  
Use -h for help.
```

DLLList

```
$ python2.7 vol.py -f ~/Downloads/jackcr-challenge/ENG-USTXHOU-148/memdump.bin --profile=WinXPSP2x86 --kdbg=0x8054cde0 dlllist -p 364
```

wc.exe pid: 364

Command line : wc.exe -e -o h.out

Service Pack 3

Base	Size	LoadCount	LoadTime	Path
0x00400000	0x38000	0xffff		C:\WINDOWS\System32\wc.exe
...				

-e: Lists logon sessions NTLM credentials indefinitely. Refreshes every time a logon event occurs

[\[https://github.com/brav0hax/smbexec/blob/master/WCE-README\]](https://github.com/brav0hax/smbexec/blob/master/WCE-README)

DLLDump/ProcDump

```
$ python2.7 vol.py -f ~/Downloads/jackcr-  
challenge/ENG-USTXHOU-148/memdump.bin --  
profile=WinXPSP2x86 --kdbg=0x8054cde0 dlldump -p  
364 --dump-dir binaries/
```

Process(V)	Name	Module Base	Module Name	Result
-----	-----	-----	-----	-----
0x82049690	wc.exe	0x000400000	wc.exe	OK: module.364.2049690.400000.dll
...				

VirusTotal

```
$ md5 module.364.2049690.4000000.dll  
MD5 (module.364.2049690.4000000.dll) =  
4a5bbe4ea1d9239b2d8cad07dd7f7090
```



58 / 68

58 engines detected this file

SHA-256	4615db3a06a2fbb2f2eeeab0cba1ff4305800088a424b110c409798c51a501ad
File name	executable.364.exe
File size	203.5 KB
Last analysis	2017-10-27 04:26:14 UTC
Community score	-53

IEHistory

```
$ python2.7 vol.py -f ~/Downloads/jackcr-  
challenge/ENG-USTXHOU-148/memdump.bin --  
profile=WinXPSP2x86 --kdbg=0x8054cde0  
iehistory
```

Process: 284 explorer.exe

Cache type "DEST" at 0xdcb69

Last modified: 2012-11-26 17:01:53 UTC+0000

Last accessed: 2012-11-26 23:01:54 UTC+0000

URL: **callb**@http://58.64.132.8/download/Symantec-1.43-1.exe

MFT

```
$ python2.7 vol.py -f ~/Downloads/jackcr-challenge/ENG-USTXHOU-148/memdump.bin  
--profile=WinXPSP2x86 --kdbg=0x8054cde0 mftparser
```

2012-11-26 23:01:38,2012-11-26 23:01:38,2012-11-26 23:01:38,2012-11-26 23:01:38,
WINDOWS\Prefetch\IEXPLO~1.PF

2012-11-26 23:01:38,2012-11-26 23:01:38,2012-11-26 23:01:38,2012-11-26
23:01:38,WINDOWS\Prefetch\IEXPLORE.EXE-27122324.pf

2012-11-26 23:01:53,2012-11-26 23:01:53,2012-11-26 23:01:53,2012-11-26 23:01:53,
Documents and Settings\callb\Local Settings\History\History.IE5\MSHIST~1

...

2004-08-18 02:00:00,2004-08-18 02:00:00,2012-11-26 23:01:54,2012-11-26 23:01:54,
WINDOWS\system32\6to4ex.dll

...

2012-11-26 23:01:54,2012-11-26 23:01:54,2012-11-26 23:01:54,2012-11-26 23:01:54,
WINDOWS\Prefetch\SYMANT~1.PF

2012-11-26 23:01:54,2012-11-26 23:01:54,2012-11-26 23:01:54,2012-11-26
23:01:54,WINDOWS\Prefetch\SYMANTEC-1.43-1[2].EXE-3793B625.pf

MFT

2012-11-26 23:03:10,2012-11-26 23:03:10,2012-11-26 23:03:10,2012-11-26 23:03:10,WINDOWS\webui
2012-11-26 23:03:21,2012-11-26 23:03:21,2012-11-26 23:03:21,2012-11-26 23:03:21,WINDOWS\Prefetch\IPCONF~1.PF
2012-11-26 23:03:21,2012-11-26 23:03:21,2012-11-26 23:03:21,2012-11-26 23:03:21,WINDOWS\Prefetch\IPCONFIG.EXE-2395F30B.pf
2012-11-26 23:06:34,2012-11-26 23:06:34,2012-11-26 23:06:34,2012-11-26 23:06:34,WINDOWS\ps.exe
2012-11-26 23:06:47,2012-11-26 23:06:47,2012-11-26 23:06:47,2012-11-26 23:06:47,WINDOWS\webui\gs.exe
2012-11-26 23:06:52,2012-11-26 23:06:52,2012-11-26 23:06:52,2012-11-26 23:06:52,WINDOWS\webui\ra.exe
2012-11-26 23:06:56,2012-11-26 23:06:56,2012-11-26 23:06:56,2012-11-26 23:06:56,WINDOWS\webui\sl.exe
2012-11-26 23:06:59,2012-11-26 23:06:59,2012-11-26 23:06:59,2012-11-26 23:06:59,WINDOWS\webui\wc.exe
2012-11-26 23:07:31,2012-11-26 23:07:31,2012-11-26 23:07:31,2012-11-26 23:07:31,WINDOWS\webui\netuse.dll
2012-11-26 23:07:53,2012-11-26 23:07:53,2012-11-26 23:07:53,2012-11-26 23:07:53,WINDOWS\Prefetch\NET.EXE-01A53C2F.pf
2012-11-26 23:08:26,2012-11-26 23:08:26,2012-11-26 23:08:26,2012-11-26 23:08:26,WINDOWS\Prefetch\NET1EX~1.PF
2012-11-26 23:10:35,2012-11-26 23:10:35,2012-11-26 23:10:35,2012-11-26 23:10:35,WINDOWS\Prefetch\SLEXE-~1.PF
2012-11-26 23:10:35,2012-11-26 23:10:35,2012-11-26 23:10:35,2012-11-26 23:10:35,WINDOWS\Prefetch\SL.EXE-010E2A23.pf
2012-11-26 23:11:58,2012-11-26 23:11:58,2012-11-26 23:11:58,2012-11-26 23:11:58,WINDOWS\Prefetch\GSEX~1.PF
2012-11-26 23:11:58,2012-11-26 23:11:58,2012-11-26 23:11:58,2012-11-26 23:11:58,WINDOWS\Prefetch\GS.EXE-3796DDD9.pf
2012-11-26 23:15:44,2012-11-26 23:15:44,2012-11-26 23:15:44,2012-11-26 23:15:44,WINDOWS\Prefetch\PINGEX~1.PF
2012-11-26 23:15:44,2012-11-26 23:15:44,2012-11-26 23:15:44,2012-11-26 23:15:44,WINDOWS\Prefetch\PING.EXE-31216D26.pf
2012-11-26 23:58:51,2012-11-26 23:58:51,2012-11-26 23:58:51,2012-11-26 23:58:51,WINDOWS\Temp\wceaux.dll
2012-11-26 23:58:51,2012-11-26 23:58:51,2012-11-26 23:58:51,2012-11-26 23:58:51,WINDOWS\Prefetch\WCEXE-~1.PF
2012-11-26 23:58:51,2012-11-26 23:58:51,2012-11-26 23:58:51,2012-11-26 23:58:51,WINDOWS\Prefetch\WC.EXE-21AD5E60.pf
2012-11-26 23:58:51,2012-11-26 23:59:04,2012-11-26 23:59:04,2012-11-26 23:59:04,WINDOWS\Temp\wceaux.dll
2012-11-27 00:00:57,2012-11-27 00:00:57,2012-11-27 00:00:57,2012-11-27 00:00:57,WINDOWS\Prefetch\PSEX~1.PF
2012-11-27 00:00:57,2012-11-27 00:00:57,2012-11-27 00:00:57,2012-11-27 00:00:57,WINDOWS\Prefetch\PS.EXE-09745CC1.pf
2012-11-27 00:10:44,2012-11-27 00:10:44,2012-11-27 00:10:44,2012-11-27 00:10:44,WINDOWS\Temp\wceaux.dll
2012-11-27 00:49:01,2012-11-27 00:49:01,2012-11-27 00:49:01,2012-11-27 00:49:01,WINDOWS\webui\system.dll
2012-11-27 00:57:20,2012-11-27 00:57:20,2012-11-27 00:57:20,2012-11-27 00:57:20,WINDOWS\webui\svchost.dll
2012-11-27 01:01:39,2012-11-27 01:01:39,2012-11-27 01:01:39,2012-11-27 01:01:39,WINDOWS\webui\https.dll
2012-11-27 01:14:48,2012-11-27 01:14:48,2012-11-27 01:14:48,2012-11-27 01:14:48,WINDOWS\webui\netstat.dll
2012-11-27 01:26:47,2012-11-27 01:26:47,2012-11-27 01:26:47,2012-11-27 01:26:47,WINDOWS\webui\system5.bat
2012-11-27 01:27:03,2012-11-27 01:27:03,2012-11-27 01:27:03,2012-11-27 01:27:03,WINDOWS\system32\wc.exe
2012-11-27 01:27:03,2012-11-27 01:27:03,2012-11-27 01:27:03,2012-11-27 01:27:03,WINDOWS\Tasks\At1.job
2012-11-27 01:27:03,2012-11-27 01:27:03,2012-11-27 01:27:03,2012-11-27 01:27:03,WINDOWS\Prefetch\ATEXE-~1.PF
2012-11-27 01:27:03,2012-11-27 01:27:03,2012-11-27 01:27:03,2012-11-27 01:27:03,WINDOWS\Prefetch\AT.EXE-2770DD18.pf
2012-11-27 01:30:00,2012-11-27 01:30:00,2012-11-27 01:30:00,2012-11-27 01:30:00,WINDOWS\system32\h.out
2012-11-27 01:30:00,2012-11-27 01:30:00,2012-11-27 01:30:00,2012-11-27 01:30:00,WINDOWS\Temp\wceaux.dll
2012-11-27 01:30:10,2012-11-27 01:30:10,2012-11-27 01:30:10,2012-11-27 01:30:10,WINDOWS\Prefetch\WCEXE-~2.PF
2012-11-27 01:30:10,2012-11-27 01:30:10,2012-11-27 01:30:10,2012-11-27 01:30:10,WINDOWS\Prefetch\WC.EXE-06BFE764.pf

MFT

WINDOWS\webui\system5.bat

\$DATA

0000000000:	40 65 63 68 6f 20 6f 66 66 0d 0a 63 6f 70 79 20	@echo.off..copy.
0000000010:	63 3a 5c 77 69 6e 64 6f 77 73 5c 77 65 62 75 69	c:\windows\webui
0000000020:	5c 77 63 2e 65 78 65 20 63 3a 5c 77 69 6e 64 6f	\wc.exe.c:\windo
0000000030:	77 73 5c 73 79 73 74 65 6d 33 32 0d 0a 61 74 20	ws\system32..at.
0000000040:	31 39 3a 33 30 20 77 63 2e 65 78 65 20 2d 65 20	19:30.wc.exe.-e.
0000000050:	2d 6f 20 68 2e 6f 75 74	-o.h.out

DumpFile

```
$ python2.7 vol.py -f ~/Downloads/jackcr-challenge/ENG-USTXHOU-148/  
memdump.bin --profile=WinXPSP2x86 --kdbg=0x8054cde0 dumpfiles --dump-  
dir=binaries/ -r 6to4ex\.dll -i -S summary.txt
```

```
ImageSectionObject 0x821e5c70 1024 \Device\HarddiskVolume1\WINDOWS\system32\6to4ex.dll  
DataSectionObject 0x821e5c70 1024 \Device\HarddiskVolume1\WINDOWS\system32\6to4ex.dll
```

```
$ md5 file.1024.0x8221c5c8.img  
MD5 (file.1024.0x8221c5c8.img) = 0ed1552f4e73f3b79a21253bac5cab35
```



54 / 59

54 engines detected this file

SHA-256	2122406e218b8fcdfb5d5331fa7cd7dea7287c600814fa8a763eb6229d39f0e7
File name	Microsoft(R) Windows(R) Operating System
File size	94 KB
Last analysis	2017-05-09 14:03:10 UTC

DumpFile All

Sophos AV

- one hit (6to4ex.dll)

VirusTotal

- 41 with >0 hits
- 4 with >4 hits (6to4ex.dll, wc.exe, wuauclt.exe)
- Additional is WINDOWS\\explorer.exe (ab227c0aaba17faf8469e9ceb6009ec7)

2012-11-23 16:32:05,2008-04-14 11:42:20,2012-11-23 16:32:06,2012-11-23 16:32:05,
WINDOWS\\explorer.exe
2012-11-23 16:45:27,2012-11-23 16:45:27,2012-11-23 16:45:27,2012-11-23 16:45:27,
WINDOWS\\Prefetch\\EXPLORER.EXE-082F38A9.pf

Grep Files

```
Security Department  
isd@petro-markets.info  
amirs@petro-market.org; callb@petro-market.org; wrightd@petro-market.org  
<amirs@petro-market.org>; <callb@petro-market.org>; <wrightd@petro-market.org>  
DC-USTXHOU.petro-market.org
```

```
amirs@petro-market.org  
[is on the phone]  
<HTML><META HTTP-EQUIV="content-type" CONTENT="text/html; charset=utf-8">  
<FONT size=2 face=Arial><A  
href="http://58.64.132.8/download/Symantec-1.43-1.exe">http://58.64.132.8/download/Symantec-1.43-1.exe</A></FONT>
```


Grep Files

URL

<http://58.64.132.8/download/Symantec-1.43-1.exe>

Symantec-1.43-1[1].exe

HTTP/1.1 200 OK

ETag: "21628-1b667-4cf2b68a20f60"

Content-Length: 112231

Keep-Alive: timeout=15, max=100

Content-Type: application/x-msdos-program

~U:callb

URL

<http://58.64.132.8/download/Symantec-1.43-1.exe>

Symantec-1.43-1[2].exe

HTTP/1.1 200 OK

ETag: "21628-1b667-4cf2b68a20f60"

Content-Length: 112231

Keep-Alive: timeout=15, max=100

Content-Type: application/x-msdos-program

~U:callb

Primary IOCs

- > 58.64.132.141
- > 58.64.132.8
- > <http://58.64.132.8/download/Symantec-1.43-1.exe>
- > Symantec-1.43-1.exe
- > 6to4ex.dll (29f63761610079940e43abd1d7c9c50ab678fef1da43c4c961069bbb8f7d0628)
- > wc.exe (4615db3a06a2fbb2f2eeeab0cba1ff4305800088a424b110c409798c51a501ad)
- > wuauclt.exe (f11d7931ae893ac103377cad7ea283cce2d405aeae18745e72d1a206177266b7)

Python Script

```
[i] Using image:  
/Users/user/Downloads/jackcr-challenge/ENG-USTXHOU-148/memdump.bin  
[i] Starting Volatility process...  
[i] Determining profile and kdbg values...  
[-] --profile: WinXPSP2x86  
[-] --kdbg: 0x8054cde0  
[i] Running selected plugins...  
[-] connscan  
[-] pstree
```

Python Script

```
[i] Checking processes...
[!] Parent process incorrect for explorer.exe (244: mdd.exe)
[i] Checking network connections...
[!] External connection - svchost.exe (1024) to 58.64.132.141:80
[!] svchost.exe connecting externally
[-] Getting child processes
[-] Found wuauclt.exe 1628
[-] Found wc.exe 364
[-] Dumping associated dlls
```

Python Script

```
# Misspelt process names
# Add misspelt process to this list
misspelt = ['scvhost', 'svhost', 'lssass', 'wsock32', 'kerne132', \
            'isass', 'nvcpl.exe', 'crss']
for name in misspelt:
    if name in process[1].lower():
        print '[!] Misspelt process name - '+process[1]+' ('+\
              process[2]+')'

# Check for parents
# Add parents to this dict
parents = { 'svchost.exe': 'services.exe', \
            'smss.exe': 'System', \
            'wininit.exe': ['', 'smss.exe'], \
            'taskhost.exe': 'services.exe', \
            'lsass.exe': ['wininit.exe', 'winlogon.exe'], \
            'winlogon.exe': ['', 'smss.exe'], \
            'iexplore.exe': 'explorer.exe', \
            'explorer.exe': ['', 'userinit.exe'], \
            'lsm.exe': 'wininit.exe', \
            'services.exe': ['wininit.exe', 'winlogon.exe'], \
            'csrss.exe': ['', 'smss.exe'] }
```

```
# Check for external IP address
internal = False
ip = connection[3]

if ip.startswith('10.'): internal = True
for i in range(16,32):
    if ip.startswith('172.'+str(i)+'.'): internal = True
if ip.startswith('172.168.'): internal = True
if ip.startswith('0.'): internal = True
if ip.startswith('127.'): internal = True
if ip.startswith('128.0.'): internal = True
if ip.startswith('169.254.'): internal = True
if ip.startswith('191.255.'): internal = True
if ip.startswith('192.0.0.'): internal = True
if ip.startswith('223.255.255.'): internal = True
```

Integration

```
[ - ] Performing Sophos AV scan  
[!] Virus 'Mal/Whybo-A' found in file  
binaries/module.1024.20b3da0.10000000.dll (6to4ex.dll)
```

```
[ - ] Performing VT lookup  
[!] f11d7931ae893ac103377cad7ea283cce2d405aeae18745e72d1a206177266b7  
(wuauclt.exe - binaries/module.1628.2045da0.400000.dll), Detections: 11  
[!] 29f63761610079940e43abd1d7c9c50ab678fef1da43c4c961069bbb8f7d0628  
(6to4ex.dll - binaries/module.1024.20b3da0.10000000.dll), Detections: 61  
[!] 4615db3a06a2fbb2f2eeeab0cba1ff4305800088a424b110c409798c51a501ad  
(wc.exe - binaries/module.364.2049690.400000.dll), Detections: 58
```

Integration

```
print '[-] Performing Sophos AV scan'
proc = subprocess.Popen(['sweep', 'binaries/'], stdout=subprocess.PIPE, \
    stderr=subprocess.PIPE)
out = proc.stdout.read()
alerts = re.findall('>>> Virus.*', out)
```

```
print '[-] Performing VT lookup - this will take some time'
proc = subprocess.Popen(['python2.7', 'virustotal-search.py', '-k', api_key, 'binaries/lookup_sha256.txt'], \
    stdout=subprocess.PIPE, stderr=subprocess.PIPE)
out = proc.stdout.read()
```

