You can see from the above that the iexplore.exe (PID 796) was spawned from svchost.exe (pid 884). If you inspected the volatility getsids output for PID 796 you will notice that iexplore.exe is running as a SYSTEM user. Both of these occurrences is very odd and not normal. Iexplore.exe should be launched from explorer.exe and should be running as a user process.

In the connsan output above, you notice that PID 796 (iexplore.exe) is connecting to a remote system on port 89. Usually http traffic is directed on port 80 or 443 only. Again this would be a very odd thing to witness for a program. This makes the iexplore.exe process very suspicious indeed.
When you examine the dlllist output for PID 796 (iexplore.exe) you will notice that there is a rogue named dll which is hard to see. Irykmmww.dll is named odd because the dll is spelled with a 1 (one) in the second letter where an l (lower case L) should be seen.

So it looks as though PID 796 is malware, but it is clear that it isn’t started normally. If you tried to see if the svchost.exe was injected it would fail and not show up. Svchost.exe is not injected. So how does the malware start on the system?
When we run the svcscan (Service Scan) plugin for volatility, we notice a driver running on the system called irykmmww which is the same named rogue dll spotted earlier. To figure out what this driver is doing, we should check driver hooking in apihooks and ssdt.

```
# vol.py -f APT.img --profile=WinXPSP3x86
ssdt | grep -v ntoskrnl | grep -v win32k
```

[x86] Gathering all referenced SSDTs from KTHREADs...
Finding appropriate address space for tables...
SSDT[0] at 80501b9c with 284 entries
  Entry 0x0042: 0xf836fe9c (NtDeviceIoControlFile) owned by irykmmww.sys
  Entry 0x0047: 0xf83706dc (NtEnumerateKey) owned by irykmmww.sys
  Entry 0x0049: 0xf837075e (NtEnumerateValueKey) owned by irykmmww.sys
  Entry 0x0077: 0xf837028f (NtOpenKey) owned by irykmmww.sys
  Entry 0x0091: 0xf8370a8c (NtQueryDirectoryFile) owned by irykmmww.sys
  Entry 0x00ad: 0xf836fe3e (NtQuerySystemInformation) owned by irykmmww.sys
  Entry 0x00b1: 0xf837091a (NtQueryValueKey) owned by irykmmww.sys
SSDT[1] at bf999d00 with 667 entries

Finally we can tell the driver irykmmww.sys is a rootkit loaded in the system. Clearly it is meant to do file hiding and more.

Here is some additional information on the IP address found earlier in our output of connscan.

**DNS INFORMATION FOR 218.85.133.23**
Excerpt from malware report on the malware.

- The malware will create the device `\Device\irykmmww (NT namespace)` and `\\.\irykmmww` ("Win32" namespace), and the driver `\Driver\irykmmww`. These will be visible with normal tools such as "Winobj".
- The malware may hide at least one instance of an `IExplore.exe` process such that it is detectable only with memory forensics.
- The malware kernel driver runs as a service named `irykmmww` with a Description of `irykmmww`.
- Files, directories, registry keys, and registry values starting with the name `irykmmww` may be hidden unless you are using memory forensics to see it.
- The DLLs `irykmmww.d1l (D-one-L)` or `irykmmww.dll` may appear in a process module listing, although the files themselves may remain hidden due to the rootkit.
- The malware will make HTTP requests to 218.85.133.23 on TCP port 89.
- The malware may make HTTP requests with the URI `/index.asp?<number>` with no User-Agent.
Additional Analysis submitted by Gebhard Zocher

Stage 1: Identify Rogue Processes

```bash
vol.py pslist:
- system boot time: 2009-04-16 16:10:01
- msiexec.exe (Windows Installer, 1464, 2009-04-16 16:11:02) started from services (704, 2009-04-16 16:10:06)
```

```bash
vol.py psscan:
- no news

vol.py pstree:
- no news
```

Stage 2: Analyze Process DLLs and Handles

```bash
vol.py dlllist -p 1464
- command line: C:\WINDOWS\system32\msiexec.exe /V
- nothing stands out

vol.py dlllist -p 704
- nothing stands out

vol.py dlllist -p 840
- nothing stands out

vol.py dlllist -p 1672
- nothing stands out

vol.py dlllist -p 456
- OK, command line shows this is obviously the MIRA Agent from Mandiant, so everything regarding 456 is not suspicious anymore

vol.py dlllist -p 796
- nothing stands out

vol.py dlllist -p 884
- command line: C:\WINDOWS\system32\svchost -k DcomLaunch

so regarding the processes we still have:
- msiexec.exe (Windows Installer, 1464, 2009-04-16 16:11:02) started from services (704, 2009-04-16 16:10:06)
- iexplore.exe (IE, 796, 2009-05-05 19:28:28) started from svchost.exe
-> mostly suspicious is the IE started from svchost 884

vol.py getsids -p 796:
Volatile Systems Volatility Framework 2.2
iexplore.exe (796): S-1-5-18 (Local System)
iexplore.exe (796): S-1-5-32-544 (Administrators)
iexplore.exe (796): S-1-1-0 (Everyone)
iexplore.exe (796): S-1-5-11 (Authenticated Users)
-> interesting, an IE running as local system ...

vol.py getsids -p 1464:
Volatile Systems Volatility Framework 2.2
msiexec.exe (1464): S-1-5-18 (Local System)
msiexec.exe (1464): S-1-5-32-544 (Administrators)
msiexec.exe (1464): S-1-1-0 (Everyone)
msiexec.exe (1464): S-1-5-11 (Authenticated Users)

vol.py handles -p 796
!!! 0x822e9578 796 0x758 0x12019f File
\Device\irykmmww
??? 0xe10096e0 796 0x7fc 0xf0003 KeyedEvent
CritSecOutOfMemoryEvent

vol.py handles -p 1464
??? 0xe10096e0 1464 0x4 0xf0003 KeyedEvent
CritSecOutOfMemoryEvent
!!! 0x822f2108 1464 0x24 0x1f0001 Mutant
SHIMLIB_LOG_MUTEX
??? 0x81e7c8e0 1464 0x3c 0x100001 File
\Device\KsecDD
??? 0x822f07750 1464 0x70 0x12019f File
\Device\NamedPipe\net\NtControlPipe13
??? 0xe1d74160 1464 0xf8 0xf003f Key
MACHINE\SOFTWARE\MICROSOFT\COM
??? 0xe1015030 1464 0x138 0x1f0001 Port
OLE6D80DE069215474C95DC80B2A50C
??? 0x821e07f0 1464 0x1a8 0x120001 Mutant
ShimCacheMutex
??? 0xe177e620 1464 0x208 0x2 Section
ShimSharedMemory
??? 0xe181a8160 1464 0x274 0x100000 Event
userenv:
Machine Group Policy has been applied
??? 0xe1f78820 1464 0x278 0x100000 Event
userenv: User
Group Policy has been applied
+ various Keys regarding certificates

vol.py filescan
-> no idea for what to grep
irykmmww
vol.py svcscan:
-> # 1464 seems to be legit, but SHIMLIB_LOG_MUTEX is suspicious
-> potentially inserted?

suspicious process:
Offset: 0x38ab98
Order: 252
Process ID: -
Service Name: irykmmww
Display Name: irykmmww
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\irykmmww

vol.py filescan | grep -i irykmmww
Volatile Systems Volatility Framework 2.2
0x01f1cd20 1 0 -W----
\Device\HarddiskVolume1???UME~1\demo\LOCALS~1\Temp\irykmmww.log
0x01f20d20 1 0 R--r-d
\Device\HarddiskVolume1\WINDOWS\system32\drivers\irykmmww.sys
0x02121e08 1 0 R--r-d
\Device\HarddiskVolume1\WINDOWS\system32\irykmmww.dll
0x02387908 1 0 R-----
\Device\HarddiskVolume1\WINDOWS\system32\irykmmww.dll
0x023beca8 1 0 R--r-d
\Device\HarddiskVolume1\WINDOWS\system32\drivers\irykmmww.sys
0x02f7cd20 1 0 R--r-d
\Device\HarddiskVolume1\WINDOWS\system32\drivers\irykmmww.sys
0x03282e08 1 0 R--r-d
\Device\HarddiskVolume1\WINDOWS\system32\drivers\irykmmww.dll
0x1347fd20 1 0 R--r-d
\Device\HarddiskVolume1\WINDOWS\system32\drivers\irykmmww.sys
\WINDOWS\system32\drivers\irykmmww.dll

Summary:
- IE 796 ran from svchost
- suspicious MS Installer process 1464
- suspicious service w/o process ID
- suspicious files:
  ???UME~1\demo\LOCALS~1\Temp\irykmmww.log
  WINDOWS\system32\drivers\irykmmww.sys
  WINDOWS\system32\drivers\irykmmww.dll

Stage 3: Review Network Artifacts

vol.py connections
0x81e611f8 192.168.157.10:1053 218.85.133.23:89 796
-> IE accessing a system in China on port 89
inetnum: 218.85.0.0 - 218.86.127.255
netname: CHINANET-FJ
descr: CHINANET Fujian province network

APT MEMORY and MALWARE CHALLENGE
is a closed connection, so should be happened before

Stage 4: Look for Evidence of Code Injection

vol.py malfind --dump-dir ./outdir/ > malfind.out
interesting pieces:

Process: explorer.exe Pid: 1672 Address: 0x2570000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

Process: explorer.exe Pid: 1672 Address: 0x1820000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

Process: explorer.exe Pid: 1672 Address: 0x1680000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

Process: explorer.exe Pid: 1672 Address: 0x1670000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6
Process: explorer.exe Pid: 1672 Address: 0x16a0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

Process: explorer.exe Pid: 1672 Address: 0x1690000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

Process: explorer.exe Pid: 1672 Address: 0x16b0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

Process: explorer.exe Pid: 1672 Address: 0x16c0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

Process: explorer.exe Pid: 1672 Address: 0x16d0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

Process: explorer.exe Pid: 1672 Address: 0x16e0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

Process: explorer.exe Pid: 1672 Address: 0x16f0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

Process: explorer.exe Pid: 1672 Address: 0x1810000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

Process: msiexec.exe Pid: 1464 Address: 0x12f0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 3, PrivateMemory: 1, Protection: 6

Process: msiexec.exe Pid: 1464 Address: 0x1350000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 3, PrivateMemory: 1, Protection: 6

vol.py ldrmodules -p 1672
    explorer.exe 0x00970000 True True True \WINDOWS\system32\itykmmww.dll

vol.py ldrmodules -p 1464
    nothing stands out

stage 5: Check for Signs of a Rootkit
**Stage 6: Dump Suspicious Processes and Drivers**

```
vol.py dlldump --dump-dir ./outdir -p 1672 -r irykmmww
Volatile Systems Volatility Framework 2.2

<table>
<thead>
<tr>
<th>Process(V) Name</th>
<th>Module Base Module Name</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>explorer.exe</td>
<td>0x000970000 irykmmww.dll</td>
<td>OK: module.1672.1fa71a8.970000.dll</td>
</tr>
</tbody>
</table>
```

md5sum outdir/module.1672.1fa71a8.970000.dll
319bff282b3046e6c85bbe0e67338c72 outdir/module.1672.1fa71a8.970000.dll
->
https://www.virustotal.com/en/file/fe9fbcc2cf6c6666d2cdd17b7665ce66fd3ba2ceec381cf4e09f2a7a3387749/analysis/

vol.py moddump --dump-dir ./outdir -r irykmmww

Volatile Systems Volatility Framework 2.2

Module Base Module Name Result
----------------- ------------------
0x0f836f000 irykmmww.sys OK: driver.f836f000.sys

md5sum outdir/driver.f836f000.sys
c8c2e11f5627f9f143152ae61c10b outdir/driver.f836f000.sys
->
https://www.virustotal.com/en/file/a80d0353c34c20a50a35771e3794de255e9030d8b7ab21ef6d1953afa692dd97/analysis/

Summary:
- System is infected with kernel driver irykmmww.sys
  (\WINDOWS\system32\drivers\irykmmww.sys, c8c2e11f5627f9f143152ae61c10b)
  which loads on startup
- explorer.exe (1672) is infected with irykmmww.dll
  (\WINDOWS\system32\irykmmww.dll, 319bff282b3046c85bee0e67338c72)
  so every user process is under control of the attacker
- explorer.exe (1672) accessed a web site in China via https
  192.168.157.10:1050 222.128.1.2:443
- IE (796) is accessing a system in China on port 89:
  192.168.157.10:1053 218.85.133.23:89
- log file may contain additional information:
  ?????UME~1\demo\LOCALS~1\Temp\irykmmww.log