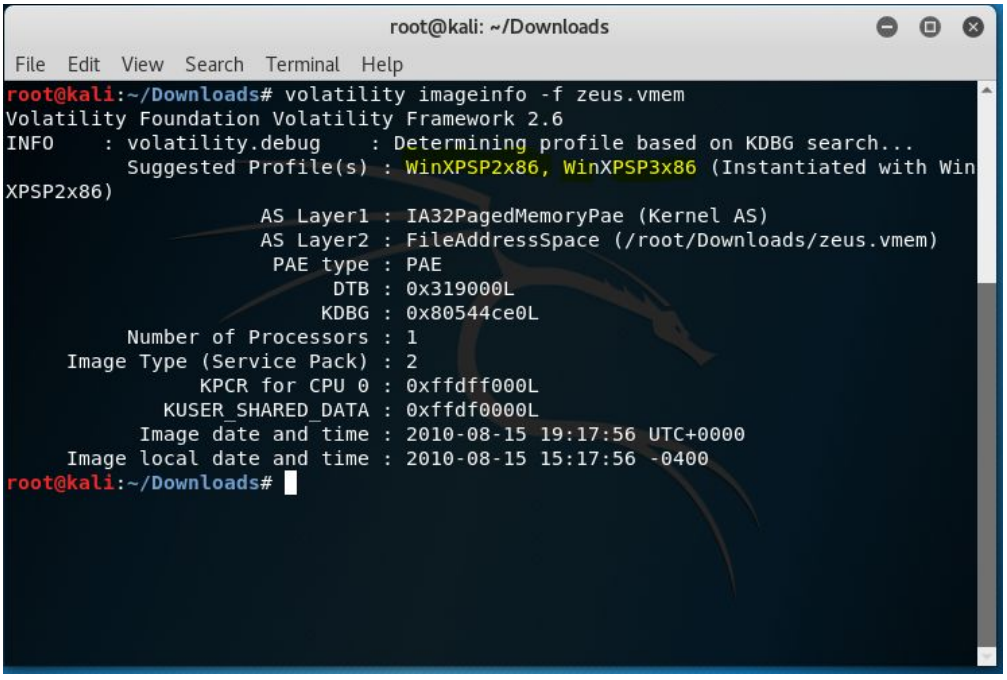
CS 5332 Digital Forensics
Texas Tech University Spring 2018

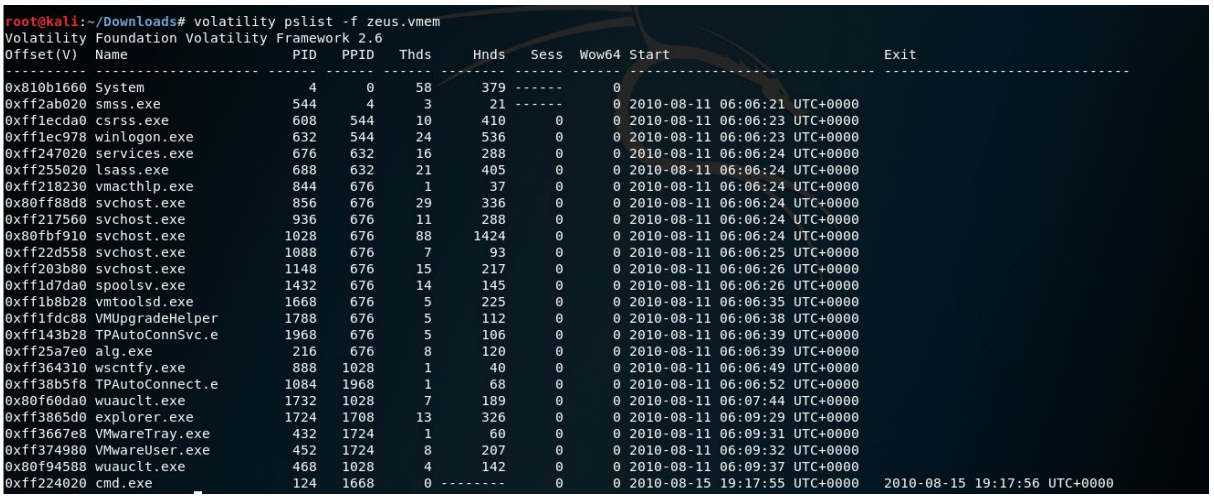
Individual Assignment 4
Rootkit
Capture the memory dump while the rootkit is running. And then report an analysis of the rootkit using volatility or any other memory forensics tool. In particular, report what the rootkit is doing and whether you are able to capture its intended target and behavior.

To find potential rootkit, I used memory dump image of Zeus malware which is used to steal bank information and carry other malicious tasks [1]. Zeus itself has embedded rootkit to hide itself to avoid detection from other security software [2]. The image of memory dump of machine that infected with Zeus can be found in this site [3]. There are some previous guide that I followed to analyze its behavior [4].

To identify the image file I used volatility command below

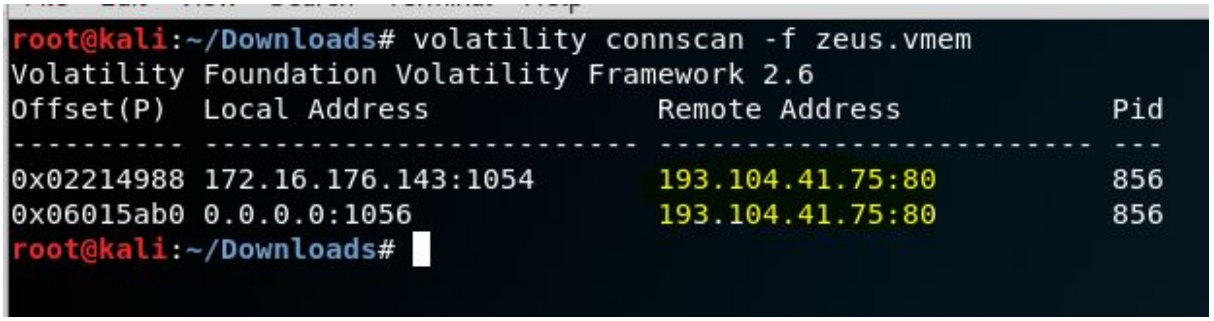


And ‘pslist’ to show all process that was running.



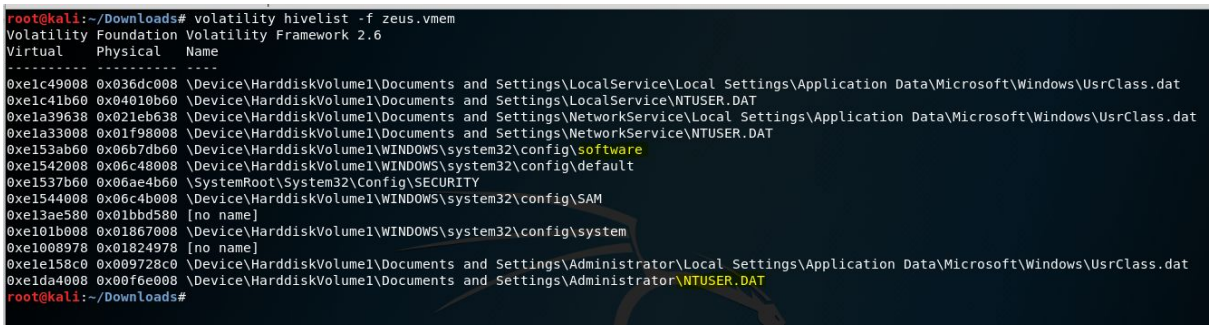
```
root@kali:~/Downloads# volatility pslist -f zeus.vmem
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x810b1660 System                    4      0     58      379 ------      0
0xff2ab020 smss.exe                544      4      3       21 ------      0 2010-08-11 06:06:21 UTC+0000
0xff1ecda0 csrss.exe               608    544     10      410      0      0 2010-08-11 06:06:23 UTC+0000
0xff1ec978 winlogon.exe            632    544     24      536      0      0 2010-08-11 06:06:23 UTC+0000
0xff247020 services.exe            676    632     16      288      0      0 2010-08-11 06:06:24 UTC+0000
0xff255020 lsass.exe               688    632     21      405      0      0 2010-08-11 06:06:24 UTC+0000
0xff218230 vmacthlp.exe            844    676      1       37      0      0 2010-08-11 06:06:24 UTC+0000
0x80ff88d8 svchost.exe             856    676     29      336      0      0 2010-08-11 06:06:24 UTC+0000
0xff217560 svchost.exe             936    676     11      288      0      0 2010-08-11 06:06:24 UTC+0000
0x80fbf910 svchost.exe            1028    676     88     1424      0      0 2010-08-11 06:06:24 UTC+0000
0xff22d558 svchost.exe            1088    676      7       93      0      0 2010-08-11 06:06:25 UTC+0000
0xff203b80 svchost.exe            1148    676     15      217      0      0 2010-08-11 06:06:26 UTC+0000
0xff1d7da0 spoolsv.exe            1432    676     14      145      0      0 2010-08-11 06:06:26 UTC+0000
0xff1b8b28 vmtoolsd.exe           1668    676      5      225      0      0 2010-08-11 06:06:35 UTC+0000
0xff1fdc88 VMUpgradeHelper        1788    676      5      112      0      0 2010-08-11 06:06:38 UTC+0000
0xff143b28 TPAutoConnSvc.e        1968    676      5      106      0      0 2010-08-11 06:06:39 UTC+0000
0xff25a7e0 alg.exe                 216    676      8      120      0      0 2010-08-11 06:06:39 UTC+0000
0xff364310 wscntfy.exe             888   1028      1       40      0      0 2010-08-11 06:06:49 UTC+0000
0xff38b5f8 TPAutoConnect.e        1084   1968      1       68      0      0 2010-08-11 06:06:52 UTC+0000
0x80f60da0 wuauclt.exe            1732   1028      7      189      0      0 2010-08-11 06:07:44 UTC+0000
0xff3865d0 explorer.exe           1724   1708     13      326      0      0 2010-08-11 06:09:29 UTC+0000
0xff3667e8 VMwareTray.exe          432   1724      1       60      0      0 2010-08-11 06:09:31 UTC+0000
0xff374980 VMwareUser.exe          452   1724      8      207      0      0 2010-08-11 06:09:32 UTC+0000
0x80f94588 wuauclt.exe             468   1028      4      142      0      0 2010-08-11 06:09:37 UTC+0000
0xff224020 cmd.exe                 124   1668      0 --------      0      0 2010-08-15 19:17:55 UTC+0000   2010-08-15 19:17:56 UTC+0000
```

‘Connscan’ is used to list all network connection. A malicious ip ‘193.104.41.75’ is captured.



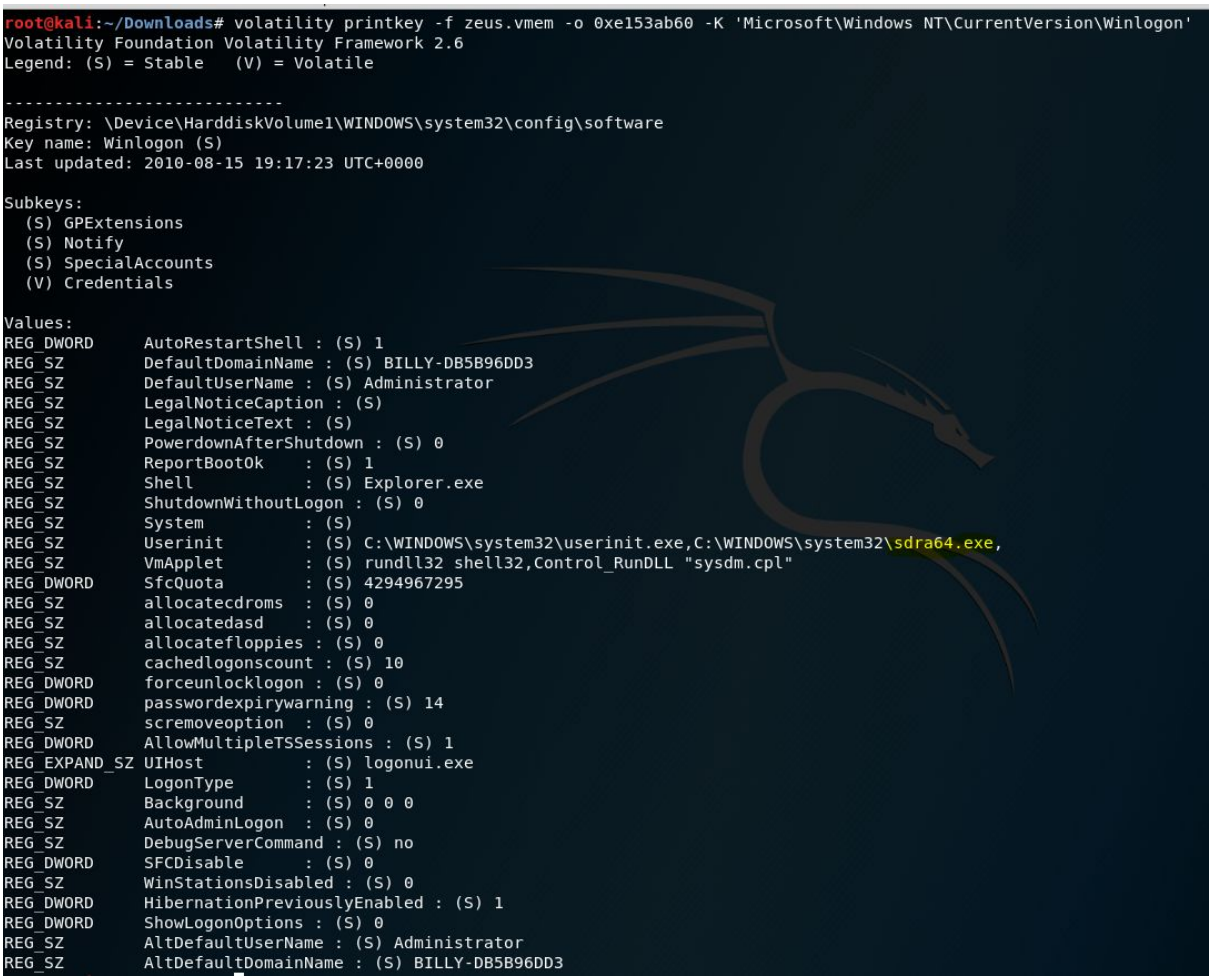
```
root@kali:~/Downloads# volatility connscan -f zeus.vmem
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x02214988 172.16.176.143:1054       193.104.41.75:80          856
0x06015ab0 0.0.0.0:1056              193.104.41.75:80          856
root@kali:~/Downloads#
```

Then virtual addresses of registry hives has to be reviewed to identify where OS keep the trace of where it kept current user’s registry.



```
root@kali:~/Downloads# volatility hivelist -f zeus.vmem
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0xe1c49008 0x036dc008 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1c41b60 0x04010b60 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe1a39638 0x021eb638 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1a33008 0x01f98008 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe153ab60 0x06b7db60 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1542008 0x06c48008 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe1537b60 0x06ae4b60 \SystemRoot\System32\Config\SECURITY
0xe1544008 0x06c4b008 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe13ae580 0x01bbd580 [no name]
0xe101b008 0x01867008 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe1008978 0x01824978 [no name]
0xe1e158c0 0x009728c0 \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1da4008 0x00f6e008 \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
root@kali:~/Downloads#
```

After that the register ‘UserInit’, is the one that is the configuration about user after login. It include personal setting, style, and also executable program that will run after login.



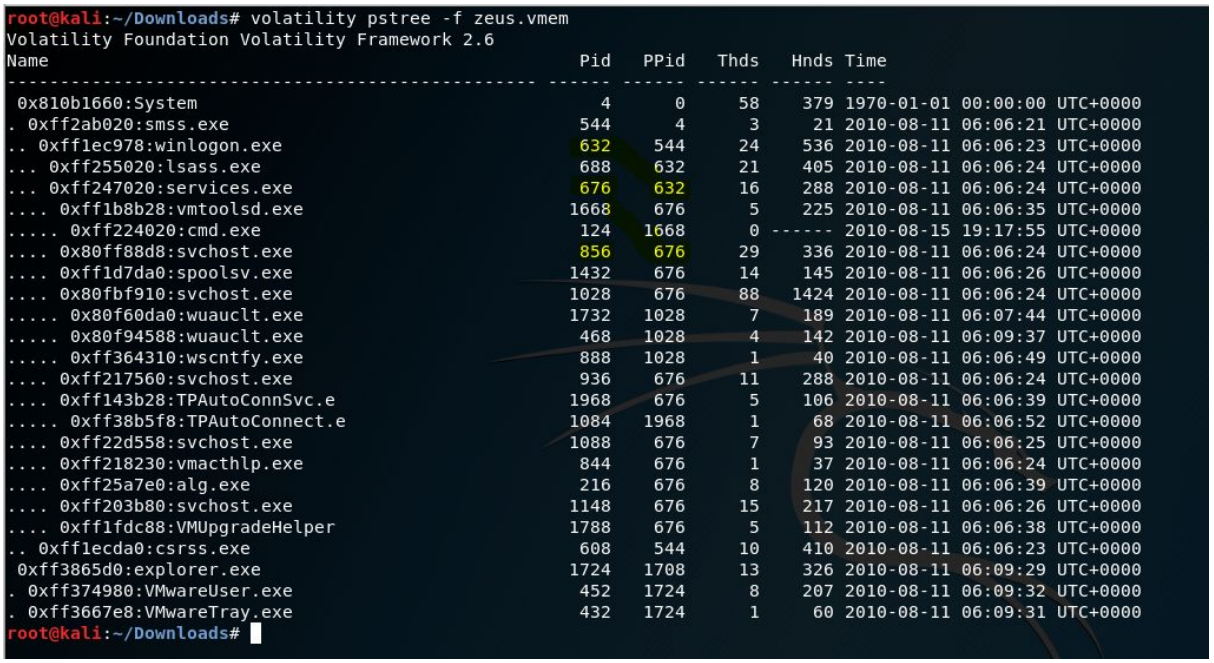
```
root@kali:~/Downloads# volatility printkey -f zeus.vmem -o 0xe153ab60 -K 'Microsoft\Windows NT\CurrentVersion\Winlogon'
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: Winlogon (S)
Last updated: 2010-08-15 19:17:23 UTC+0000

Subkeys:
  (S) GPExtensions
  (S) Notify
  (S) SpecialAccounts
  (V) Credentials

Values:
REG_DWORD     AutoRestartShell : (S) 1
REG_SZ        DefaultDomainName : (S) BILLY-DB5B96DD3
REG_SZ        DefaultUserName : (S) Administrator
REG_SZ        LegalNoticeCaption : (S)
REG_SZ        LegalNoticeText : (S)
REG_SZ        PowerdownAfterShutdown : (S) 0
REG_SZ        ReportBootOk    : (S) 1
REG_SZ        Shell           : (S) Explorer.exe
REG_SZ        ShutdownWithoutLogon : (S) 0
REG_SZ        System          : (S)
REG_SZ        Userinit        : (S) C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.exe,
REG_SZ        VmApplet        : (S) rundll32 shell32,Control_RunDLL "sysdm.cpl"
REG_DWORD     SfcQuota        : (S) 4294967295
REG_SZ        allocatecdroms  : (S) 0
REG_SZ        allocatedasd    : (S) 0
REG_SZ        allocatefloppies : (S) 0
REG_SZ        cachedlogonscount : (S) 10
REG_DWORD     forceunlocklogon : (S) 0
REG_DWORD     passwordexpirywarning : (S) 14
REG_SZ        scremoveoption  : (S) 0
REG_DWORD     AllowMultipleTSSessions : (S) 1
REG_EXPAND_SZ UIHost          : (S) logonui.exe
REG_DWORD     LogonType       : (S) 1
REG_SZ        Background      : (S) 0 0 0
REG_SZ        AutoAdminLogon  : (S) 0
REG_SZ        DebugServerCommand : (S) no
REG_DWORD     SFCDisable      : (S) 0
REG_SZ        WinStationsDisabled : (S) 0
REG_DWORD     HibernationPreviouslyEnabled : (S) 1
REG_DWORD     ShowLogonOptions : (S) 0
REG_SZ        AltDefaultUserName : (S) Administrator
REG_SZ        AltDefaultDomainName : (S) BILLY-DB5B96DD3
```

‘Pstree’ command is used to view process list as a tree so each process can be identified where it belong to.



```
root@kali:~/Downloads# volatility pstree -f zeus.vmem
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x810b1660:System                                      4      0     58    379 1970-01-01 00:00:00 UTC+0000
. 0xff2ab020:smss.exe                                 544      4      3     21 2010-08-11 06:06:21 UTC+0000
.. 0xff1ec978:winlogon.exe                            632    544     24    536 2010-08-11 06:06:23 UTC+0000
... 0xff255020:lsass.exe                              688    632     21    405 2010-08-11 06:06:24 UTC+0000
... 0xff247020:services.exe                           676    632     16    288 2010-08-11 06:06:24 UTC+0000
.... 0xff1b8b28:vmtoolsd.exe                         1668    676      5    225 2010-08-11 06:06:35 UTC+0000
..... 0xff224020:cmd.exe                              124   1668      0 ------ 2010-08-15 19:17:55 UTC+0000
.... 0x80ff88d8:svchost.exe                           856    676     29    336 2010-08-11 06:06:24 UTC+0000
.... 0xff1d7da0:spoolsv.exe                          1432    676     14    145 2010-08-11 06:06:26 UTC+0000
.... 0x80fbf910:svchost.exe                          1028    676     88   1424 2010-08-11 06:06:24 UTC+0000
..... 0x80f60da0:wuauclt.exe                         1732   1028      7    189 2010-08-11 06:07:44 UTC+0000
..... 0x80f94588:wuauclt.exe                          468   1028      4    142 2010-08-11 06:09:37 UTC+0000
..... 0xff364310:wscntfy.exe                          888   1028      1     40 2010-08-11 06:06:49 UTC+0000
.... 0xff217560:svchost.exe                           936    676     11    288 2010-08-11 06:06:24 UTC+0000
.... 0xff143b28:TPAutoConnSvc.e                      1968    676      5    106 2010-08-11 06:06:39 UTC+0000
..... 0xff38b5f8:TPAutoConnect.e                     1084   1968      1     68 2010-08-11 06:06:52 UTC+0000
.... 0xff22d558:svchost.exe                          1088    676      7     93 2010-08-11 06:06:25 UTC+0000
.... 0xff218230:vmacthlp.exe                          844    676      1     37 2010-08-11 06:06:24 UTC+0000
.... 0xff25a7e0:alg.exe                               216    676      8    120 2010-08-11 06:06:39 UTC+0000
.... 0xff203b80:svchost.exe                          1148    676     15    217 2010-08-11 06:06:26 UTC+0000
.... 0xff1fdc88:VMUpgradeHelper                      1788    676      5    112 2010-08-11 06:06:38 UTC+0000
.. 0xff1ecda0:csrss.exe                               608    544     10    410 2010-08-11 06:06:23 UTC+0000
 0xff3865d0:explorer.exe                             1724   1708     13    326 2010-08-11 06:09:29 UTC+0000
. 0xff374980:VMwareUser.exe                           452   1724      8    207 2010-08-11 06:09:32 UTC+0000
. 0xff3667e8:VMwareTray.exe                           432   1724      1     60 2010-08-11 06:09:31 UTC+0000
root@kali:~/Downloads#
```

From the result above, after winlogon(Pid 632) it call services.exe (Pid 676) which call svchost.exe (Pid 856)
The firewall of this machine is also setted to be disable.

```
root@kali:~/Downloads# volatility printkey -f zeus.vmem -K 'ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile'
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\system
Key name: StandardProfile (S)
Last updated: 2010-08-15 19:17:24 UTC+0000

Subkeys:
  (S) AuthorizedApplications

Values:
REG_DWORD     EnableFirewall  : (S) 0
```

By checking with apihook plugin, two hooking is found on process Pid 856

```
root@kali:~/Downloads# volatility apihooks -f zeus.vmem -p 856
Volatility Foundation Volatility Framework 2.6
**********************************************************************
Hook mode: Usermode
Hook type: Inline/Trampoline
Process: 856 (svchost.exe)
Victim module: ntdll.dll (0x7c900000 - 0x7c9b0000)
Function: ntdll.dll!NtCreateThread at 0x7c90d7d2
Hook address: 0xb73b47
Hooking module: <unknown>

Disassembly(0):
0x7c90d7d2 e970632684       JMP 0xb73b47
0x7c90d7d7 ba0003fe7f       MOV EDX, 0x7ffe0300
0x7c90d7dc ff12             CALL DWORD [EDX]
0x7c90d7de c22000           RET 0x20
0x7c90d7e1 90               NOP
0x7c90d7e2 90               NOP
0x7c90d7e3 90               NOP
0x7c90d7e4 90               NOP
0x7c90d7e5 90               NOP
0x7c90d7e6 90               NOP
0x7c90d7e7 b8               DB 0xb8
0x7c90d7e8 36               DB 0x36
0x7c90d7e9 00               DB 0x0

Disassembly(1):
0xb73b47 55              PUSH EBP
0xb73b48 8bec            MOV EBP, ESP
0xb73b4a 83ec18          SUB ESP, 0x18
0xb73b4d 53              PUSH EBX
0xb73b4e 56              PUSH ESI
0xb73b4f 57              PUSH EDI
0xb73b50 8b7d14          MOV EDI, [EBP+0x14]
0xb73b53 8d4514          LEA EAX, [EBP+0x14]
0xb73b56 50              PUSH EAX
0xb73b57 6a18            PUSH 0x18
0xb73b59 8d45e8          LEA EAX, [EBP-0x18]
0xb73b5c 50              PUSH EAX
0xb73b5d 33f6            XOR ESI, ESI

**********************************************************************
```

```
**********************************************************************
Hook mode: Usermode
Hook type: Inline/Trampoline
Process: 856 (svchost.exe)
Victim module: ntdll.dll (0x7c900000 - 0x7c9b0000)
Function: ntdll.dll!ZwCreateThread at 0x7c90d7d2
Hook address: 0xb73b47
Hooking module: <unknown>

Disassembly(0):
0x7c90d7d2 e970632684       JMP 0xb73b47
0x7c90d7d7 ba0003fe7f       MOV EDX, 0x7ffe0300
0x7c90d7dc ff12             CALL DWORD [EDX]
0x7c90d7de c22000           RET 0x20
0x7c90d7e1 90               NOP
0x7c90d7e2 90               NOP
0x7c90d7e3 90               NOP
0x7c90d7e4 90               NOP
0x7c90d7e5 90               NOP
0x7c90d7e6 90               NOP
0x7c90d7e7 b8               DB 0xb8
0x7c90d7e8 36               DB 0x36
0x7c90d7e9 00               DB 0x0

Disassembly(1):
0xb73b47 55              PUSH EBP
0xb73b48 8bec            MOV EBP, ESP
0xb73b4a 83ec18          SUB ESP, 0x18
0xb73b4d 53              PUSH EBX
0xb73b4e 56              PUSH ESI
0xb73b4f 57              PUSH EDI
0xb73b50 8b7d14          MOV EDI, [EBP+0x14]
0xb73b53 8d4514          LEA EAX, [EBP+0x14]
0xb73b56 50              PUSH EAX
0xb73b57 6a18            PUSH 0x18
0xb73b59 8d45e8          LEA EAX, [EBP-0x18]
0xb73b5c 50              PUSH EAX
0xb73b5d 33f6            XOR ESI, ESI
```

Conclusion

Zeus malware try to communicate with malicious ip '193.104.41.75'. This malicious executable command is placed on the Windows' logon registry that will execute after the user login. During this process, it also use rootkit to perform hooking to do other malicious task.

Reference

1. https://en.wikipedia.org/wiki/Zeus_(malware)
2. https://www.infosecurity-magazine.com/news/zeus-trojan-gets-persistent-with-new-rootkit/
3. https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples
4. https://www.evild3ad.com/956/volatility-memory-forensics-basic-usage-for-malware-analysis/