Memory Forensics

Assignment 4

Windows Registry Rootkit

Rootkit uses a vulnerability in win32k.sys by implementing the buffer overflow function. The features of this rootkit are:

- It is an NDIS based network backdoor.
- In order to avoid unknown executable code detection, it moves in the memory over discardable sections of some default Windows drivers.
- Completely undetectable by public anti-rootkit tools.
- Working on Windows 7 (SP0, SP1) x86.

Analysis

The source code is download from GitHub and the rootkit is installed by running the installer file(WindowsRegistryRootkit/bin/rootkit_installer.exe). After running this we can observe there will be a slight difference in the appearance of the windows screen. Also, we can observe the mouse intercepts. From this, we can understand that the rootkit started working. We observe these changes due to the implementation of buffer overflow functionality. (I could not capture the screen as I did on another computer)

Next, install DumpIt and capture the memory. The steps to follow the memory dump are

>cd DumpIt

>cd DumpIt.exe

The memory is captured and the .raw file is stored in DumpIt folder.

Using volatility framework 2.6 to analyze the mem.raw file,

1. Finding the image information using image info,

```
C:\Users\sunandha\Desktop\forensics\Ass1\Ass4\vol\volatility_2.6_win64_standalone>volatility_2.6_win64
_standalone.exe -f C:\Users\sunandha\Desktop\forensics\Ass1\Ass4\vol\mem.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\sunandha\Desktop\forensics\Ass1\Ass4\vol\m
em.raw)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82740c28L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82741c00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2018-05-07 05:24:52 UTC+0000
     Image local date and time : 2018-05-06 22:24:52 -0700
```

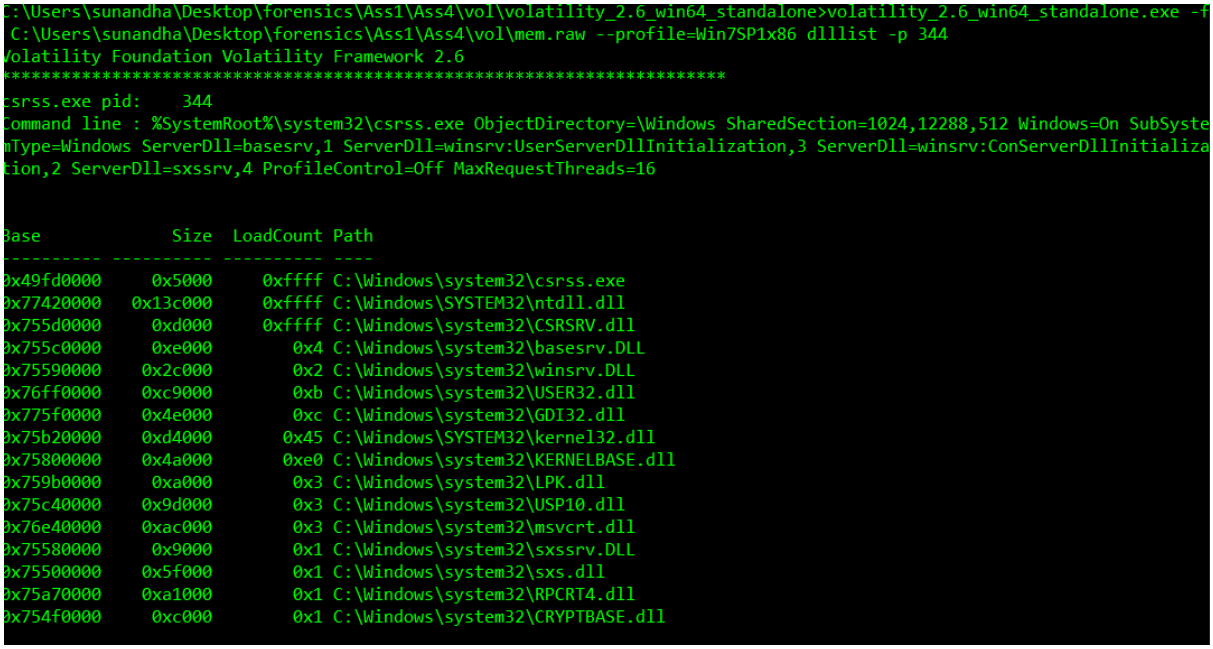
2. Find the process list using pslist. It shows a high level view of the process.

Here, the csrss.exe is the process that initializes the root. And other services.exe are the other processes of the rootkit.

```
C:\Users\sunandha\Desktop\forensics\Ass1\Ass4\vol\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f
 C:\Users\sunandha\Desktop\forensics\Ass1\Ass4\vol\mem.raw --profile=Win7SP1x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------
-----------------
0x84212798 System                    4      0     79      545 ------      0 2018-05-04 06:43:47 UTC+0000

0x85754830 smss.exe                268      4      2       29 ------      0 2018-05-04 06:43:47 UTC+0000

0x858b7d40 csrss.exe               344    328      9      451      0      0 2018-05-04 06:43:48 UTC+0000

0x85175a58 wininit.exe             380    328      3       76      0      0 2018-05-04 06:43:48 UTC+0000

0x85176928 csrss.exe               388    372      7      198      1      0 2018-05-04 06:43:48 UTC+0000

0x8595c610 services.exe            444    380     12      207      0      0 2018-05-04 06:43:48 UTC+0000

0x85976870 lsass.exe               452    380      8      559      0      0 2018-05-04 06:43:48 UTC+0000

0x85978b90 lsm.exe                 460    380     10      145      0      0 2018-05-04 06:43:48 UTC+0000

0x85977b90 winlogon.exe            472    372      5      117      1      0 2018-05-04 06:43:48 UTC+0000

0x859f1a18 svchost.exe             592    444     10      358      0      0 2018-05-04 06:43:49 UTC+0000

0x85a0a150 VBoxService.ex          656    444     12      117      0      0 2018-05-04 06:43:49 UTC+0000

0x85971d40 svchost.exe             708    444      9      287      0      0 2018-05-04 04:43:50 UTC+0000

0x85a368f0 svchost.exe             776    444     20      456      0      0 2018-05-04 04:43:50 UTC+0000

0x85a63b48 svchost.exe             880    444     24      454      0      0 2018-05-04 04:43:50 UTC+0000

0x85a6b9c0 svchost.exe             916    444     47     2467      0      0 2018-05-04 04:43:50 UTC+0000

0x85a75100 audiodg.exe             980    776      6      130      0      0 2018-05-04 04:43:50 UTC+0000
0x85c34d40 taskeng.exe            1980    916      4       79      0      0 2018-05-04 04:43:55 UTC+0000

0x85c47d40 dwm.exe                1992    880      3       71      1      0 2018-05-04 04:43:55 UTC+0000

0x85c41358 explorer.exe           2012   1972     36      968      1      0 2018-05-04 04:43:55 UTC+0000

0x86b823d0 VBoxTray.exe           1508   2012     13      154      1      0 2018-05-04 04:43:55 UTC+0000

0x85cb6030 GoogleCrashHan         2004   1584      6       94      0      0 2018-05-04 04:43:55 UTC+0000

0x851215d0 SearchIndexer.         2036    444     11      617      0      0 2018-05-04 04:44:01 UTC+0000

0x85b8f7e0 wmpnetwk.exe           1352    444      9      212      0      0 2018-05-04 04:44:01 UTC+0000

0x84fd25d8 WmiPrvSE.exe           2784    592      6      116      0      0 2018-05-04 04:44:52 UTC+0000

0x84320b30 mscorsvw.exe           3960    444      6       76      0      0 2018-05-04 21:04:45 UTC+0000

0x843aa030 sppsvc.exe             4088    444      4      147      0      0 2018-05-04 21:04:46 UTC+0000

0x843ef680 svchost.exe            1580    444     11      308      0      0 2018-05-04 21:04:46 UTC+0000

0x843ae9c0 WmiPrvSE.exe            860    592      8      185      0      0 2018-05-04 21:04:47 UTC+0000

0x85251030 TrustedInstall         2420    444      9      399      0      0 2018-05-04 21:05:32 UTC+0000

0x86af0438 SearchProtocol          144   2036      7      328      0      0 2018-05-04 21:05:51 UTC+0000

0x8598bb50 SearchFilterHo         2664   2036      5      105      0      0 2018-05-04 21:05:54 UTC+0000

0x85c477b8 rootkit_instal         2824   2012      1       72      1      0 2018-05-04 21:06:03 UTC+0000

0x84386bf8 conhost.exe            2132    388      2       53      1      0 2018-05-04 21:06:03 UTC+0000

0x85afe4c0 WMIADAP.exe            2084    916      6       89      0      0 2018-05-04 21:06:45 UTC+0000

0x84958798 DumpIt.exe             2800   2012      2       39      1      0 2018-05-04 21:07:36 UTC+0000

0x847f6ac8 conhost.exe            3384    388      2       54      1      0 2018-05-04 21:07:36 UTC+0000
```

3. Extracting the dll list of process csrss.exe using dlllist

Dlllist -processid gives the list of loaded dlls by that process.

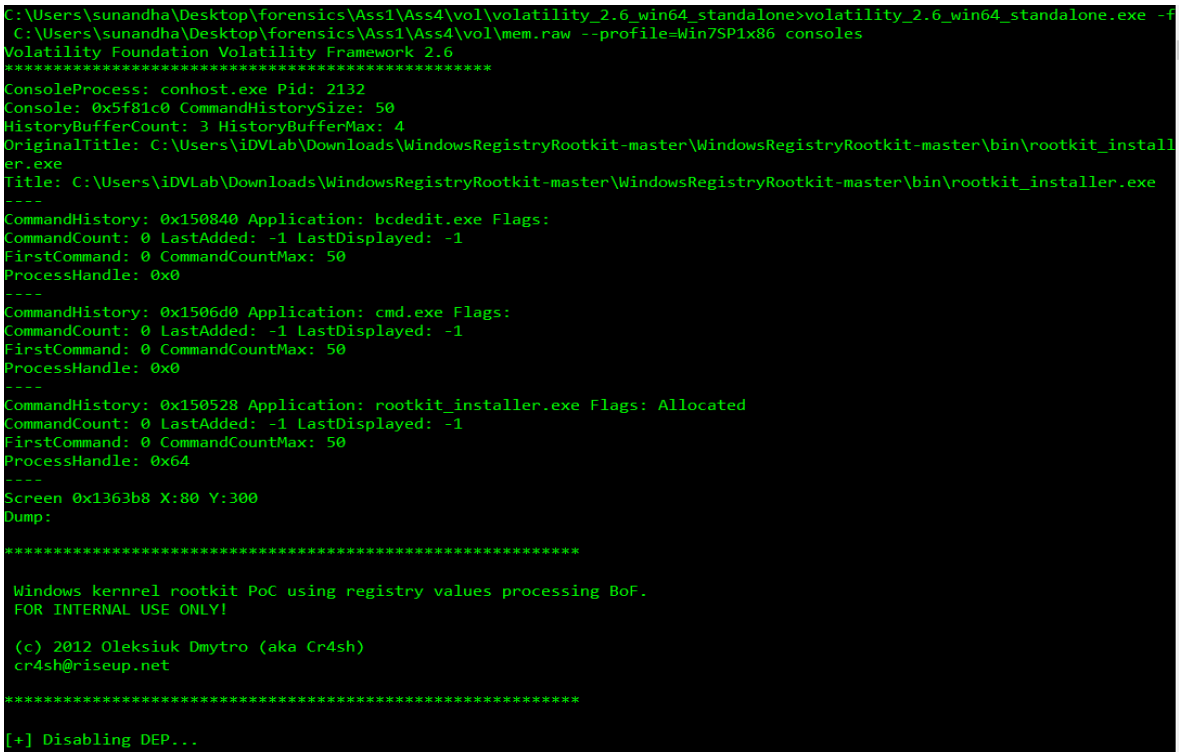


```
C:\Users\sunandha\Desktop\forensics\Ass1\Ass4\vol\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f
 C:\Users\sunandha\Desktop\forensics\Ass1\Ass4\vol\mem.raw --profile=Win7SP1x86 dlllist -p 344
Volatility Foundation Volatility Framework 2.6
************************************************************************
csrss.exe pid:    344
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,12288,512 Windows=On SubSyste
mType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitializa
tion,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16


Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x49fd0000     0x5000     0xffff C:\Windows\system32\csrss.exe
0x77420000   0x13c000     0xffff C:\Windows\SYSTEM32\ntdll.dll
0x755d0000     0xd000     0xffff C:\Windows\system32\CSRSRV.dll
0x755c0000     0xe000        0x4 C:\Windows\system32\basesrv.DLL
0x75590000     0x2c000        0x2 C:\Windows\system32\winsrv.DLL
0x76ff0000     0xc9000        0xb C:\Windows\system32\USER32.dll
0x775f0000     0x4e000        0xc C:\Windows\system32\GDI32.dll
0x75b20000     0xd4000       0x45 C:\Windows\SYSTEM32\kernel32.dll
0x75800000     0x4a000       0xe0 C:\Windows\system32\KERNELBASE.dll
0x759b0000     0xa000        0x3 C:\Windows\system32\LPK.dll
0x75c40000     0x9d000        0x3 C:\Windows\system32\USP10.dll
0x76e40000     0xac000        0x3 C:\Windows\system32\msvcrt.dll
0x75580000     0x9000        0x1 C:\Windows\system32\sxssrv.DLL
0x75500000     0x5f000        0x1 C:\Windows\system32\sxs.dll
0x75a70000     0xa1000        0x1 C:\Windows\system32\RPCRT4.dll
0x754f0000     0xc000        0x1 C:\Windows\system32\CRYPTBASE.dll
```

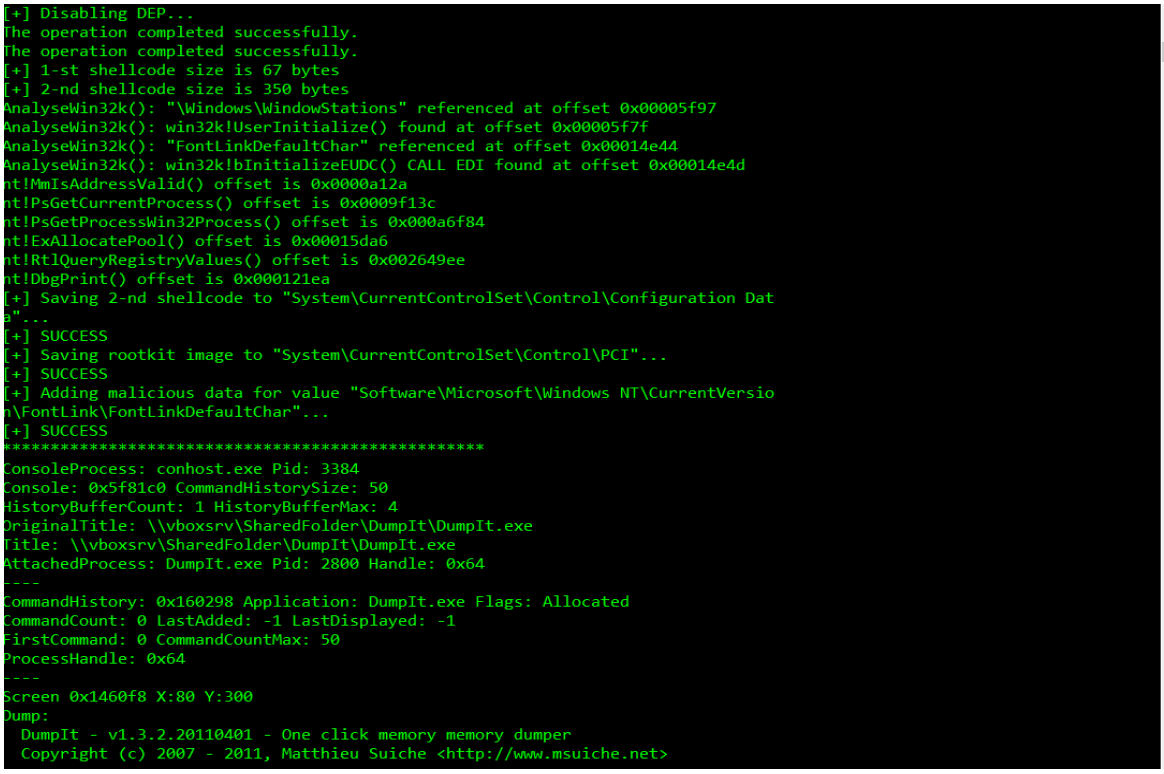
These are the dll libraries that are loaded by this process.

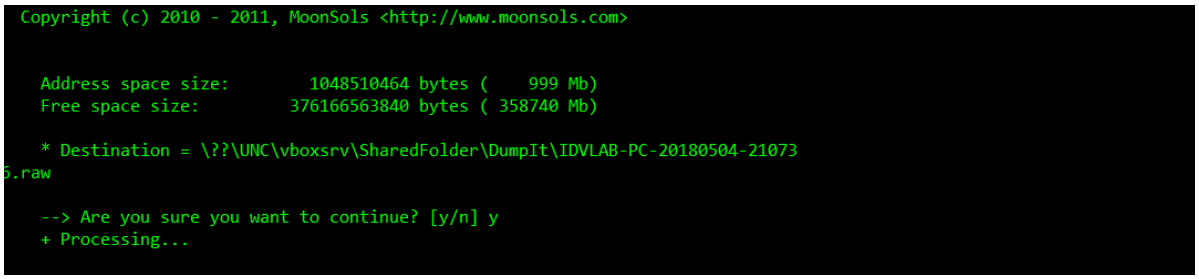
4. Finding out what processes are executed in the background using consoles command.

Consoles/cmdscan commad scan for the console information.



```
C:\Users\sunandha\Desktop\forensics\Ass1\Ass4\vol\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f
 C:\Users\sunandha\Desktop\forensics\Ass1\Ass4\vol\mem.raw --profile=Win7SP1x86 consoles
Volatility Foundation Volatility Framework 2.6
**************************************************
ConsoleProcess: conhost.exe Pid: 2132
Console: 0x5f81c0 CommandHistorySize: 50
HistoryBufferCount: 3 HistoryBufferMax: 4
OriginalTitle: C:\Users\iDVLab\Downloads\WindowsRegistryRootkit-master\WindowsRegistryRootkit-master\bin\rootkit_install
er.exe
Title: C:\Users\iDVLab\Downloads\WindowsRegistryRootkit-master\WindowsRegistryRootkit-master\bin\rootkit_installer.exe
----
CommandHistory: 0x150840 Application: bcdedit.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0x1506d0 Application: cmd.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0x150528 Application: rootkit_installer.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x64
----
Screen 0x1363b8 X:80 Y:300
Dump:

******************************************************

 Windows kernrel rootkit PoC using registry values processing BoF.
 FOR INTERNAL USE ONLY!

 (c) 2012 Oleksiuk Dmytro (aka Cr4sh)
 cr4sh@riseup.net

******************************************************

[+] Disabling DEP...
```





The second screenshot of console output shows 1st shellcode, 2nd shellcode are executed. And then it shows AnalyseWin32k(), which is the one that rootkit uses for vulnerability. Later, it is shown as

Saving 2-nd shellcode to “System\CurrentControlSet\Control\Configuration Data”

SUCCESS

Saving rootkit image to “System\CurrentControlSet\Contril\PCI”…

SUCCESS

Adding malicious data for value “Software\Microsoft\Windows NT\CurrentVersion\FontLinkDefaultChar”…

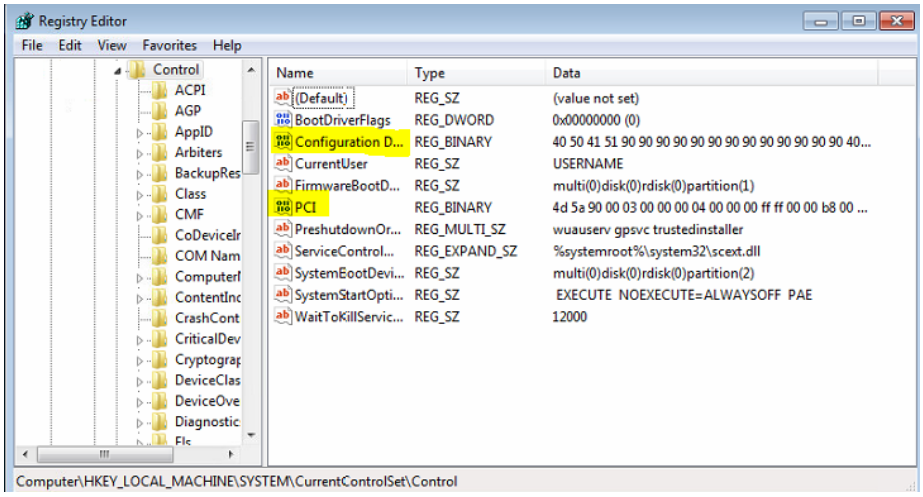
SUCCESS

5. We need to look into the registry of that windows profile. There is one command to dump the registry using volatility.

>volatitility.exe memory.raw –profile=” “ dumpregistry –dump-dir=”output folder path”

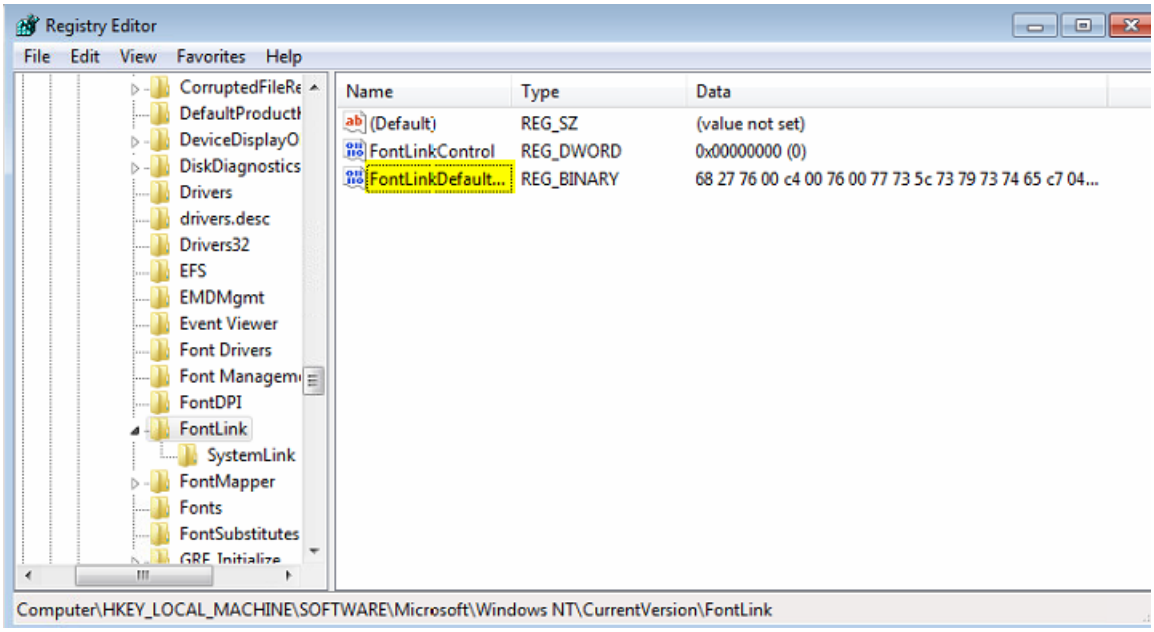
The registry files are then exported to the output folder. But there should be a registry file viewer to open these files.

Instead, I tried to check the registry in the infected windows.



“System\CurrentControlSet\Control\Configuration Data”

“System\CurrentControlSet\Contril\PCI”



“Software\Microsoft\Windows NT\CurrentVersion\FontLinkDefaultChar”

Now, export the configurationData.reg, PCI.reg, FontLinkDefaultChar.reg registry files. When these files are tried to open using text editors, it contains some registry hex code. A decoder is required to decode the registry hex to ASCII.

There is one tool called RegToText that decodes the registry hex to text.

Download the RegToText.exe file.

>RegToText.exe inputfile.reg /o:Outputfile.txt /e:ASCII

Converting, configurationData.reg file to text file.

```
C:\Users\pshra\Desktop\SUNU\VB>RegToText.exe  C:\Users\pshra\Desktop\SUNU\VB\reg-confi
g.reg /o:C:\Users\pshra\Desktop\SUNU\VB\config1.txt /e:ASCII
Selected encoding with ASCII
Reading file C:\Users\pshra\Desktop\SUNU\VB\reg-config.reg
Valid windows registry header.
Writing chunk number (@ 20 lines each)
1
Processed entire file.
Success.

Wrote out 13 lines.
Processed 1 subkeys paths and 10 key/value pairs.
Runtime: 213 milliseconds

Input  file: C:\Users\pshra\Desktop\SUNU\VB\reg-config.reg
Output file: C:\Users\pshra\Desktop\SUNU\VB\config1.txt

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
This is unlicensed "demo" software and is provided "AS IS", WITHOUT WARRANTY OF
ANY KIND.

Read Full License Agreement use /l
OR pipe 'regtotext /l > RTTLic.txt' to read license in Notepad.

For a fully licensed version of this software, contact metadataconsult@gmail.com

This unlicensed “demo” version is provided for demonstration purposes only.
Unlicensed “demo” version is limited to read and translate a few lines. You can
use this software to showcase the product to others customers. You may not leave
the product with a customer after a demonstration has been completed.

NOTE: This unlicensed “demo” version will open a blog page on each run! Licensed
version will stop this action.
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
```

config1 - Notepad

File Edit Format View Help

```
RegtoText Windows Registry Conversion Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control]
"PreshutdownOrder"=[REG_MULTI_SZ] wuauserv gpsvc trustedinstaller
"WaitToKillServiceTimeout"="12000"
"CurrentUser"="USERNAME"
"BootDriverFlags"=[REG_DWORD] 0
"ServiceControlManagerExtension"=[REG_EXPAND_SZ] %systemroot%\system32\scext.dll
"SystemStartOptions"=" EXECUTE  NOEXECUTE=ALWAYSOFF  PAE"
"SystemBootDevice"="multi(0)disk(0)rdisk(0)partition(2)"
"FirmwareBootDevice"="multi(0)disk(0)rdisk(0)partition(1)"
"Configuration Data"=[REG_BINARY:<UTF16-LE,2-byte>] ((j8Bjh}u((*(PPCI!
"PCI"=[REG_BINARY:<UTF16-LE,2-byte>] @.$L0A<h@t a@ @XdBogusProtoxNxxxC!xNx"xtTCPIPxxdwinlogon.exed!xx)x\HTTP.sys
\mrxsmb.sys\mrxsmb10.sys\mrxsmb20.sys\srv.sys\srv2.sys
\secdrv.sysxxhal.dllntoskrnl.exehal.dllhalacpi.dllhalapic.dllhalmps.dllhalaacpi.dllhalmacpi.dllntoskrnl.exentkrnlpa
.exentkrnlmp.exentkrpamp.exeH bjpP ---oE280xp@]xQE]GEutuDuG>?$Etjj-t EjM1tju(}UEMUMU,%Mh0E&jEBTQsHElMj,%jjjjhMjjj
EMUh0RHAABH-jjjM@jjj-|jjh$j<jj6}--(uu4uu8u@-tM$,%EQtH9t:vj5BMjMUEU`UE9t:vjmQjjjjjMUE9:jUMUEjjEEBHB-tj-!EUEMUUt-
jEMUUEMM~j-=..}ttQHttQHTUvH1H4"4Mj#$jjtj=.uE+uT.~..HD.A...-ELutEQMtMzHEBEuMLtEHEtEy%tEUHBj<j"( $ek4Pdx-j-}E-EUDTju\
AtHHjEE hMtUEMEEU□E|ME}MMUUEBxtEEEUMUU (`jjT'jtj jttjQuB.Hu@.$LP@NPptv @a+@@$ j |\  j !h0+j+!jjh t !jjh"<"(""j $vv
$$$j$ $ #$ jjjjt  ##|#jj $# $##j  tj$$ ap.pmppdpdp.pmpp"pdp).fWeCedtT{cdZse;:e AA^`lyRJ2&kjhjhj9Eh..MU.hu-j-.
+.....-.jjj|U4MEj-PMEHBJtQQJtQ;UMHDsUQUU<_*gA%gy~yXeBHtc9s4rtTnjfi1de@[gilX
```

Converting the pci.reg file to text,

```
C:\Users\pshra\Desktop\SUNU\VB>RegToText.exe  C:\Users\pshra\Desktop\SUNU\VB\reg-pci.r
eg /o:C:\Users\pshra\Desktop\SUNU\VB\pci1.txt /e:ASCII
Selected encoding with ASCII
Reading file C:\Users\pshra\Desktop\SUNU\VB\reg-pci.reg
Valid windows registry header.
Writing chunk number (@ 20 lines each)
1
Processed entire file.
Success.

Wrote out 13 lines.
Processed 1 subkeys paths and 10 key/value pairs.
Runtime: 207 milliseconds

Input  file: C:\Users\pshra\Desktop\SUNU\VB\reg-pci.reg
Output file: C:\Users\pshra\Desktop\SUNU\VB\pci1.txt

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
This is unlicensed "demo" software and is provided "AS IS", WITHOUT WARRANTY OF
ANY KIND.

Read Full License Agreement use /l
OR pipe 'regtotext /l > RTTLic.txt' to read license in Notepad.

For a fully licensed version of this software, contact metadataconsult@gmail.com

This unlicensed “demo” version is provided for demonstration purposes only.
Unlicensed “demo” version is limited to read and translate a few lines. You can
use this software to showcase the product to others customers. You may not leave
the product with a customer after a demonstration has been completed.

NOTE: This unlicensed “demo” version will open a blog page on each run! Licensed
version will stop this action.
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
```

Converting, DefaultChar.reg file to text,

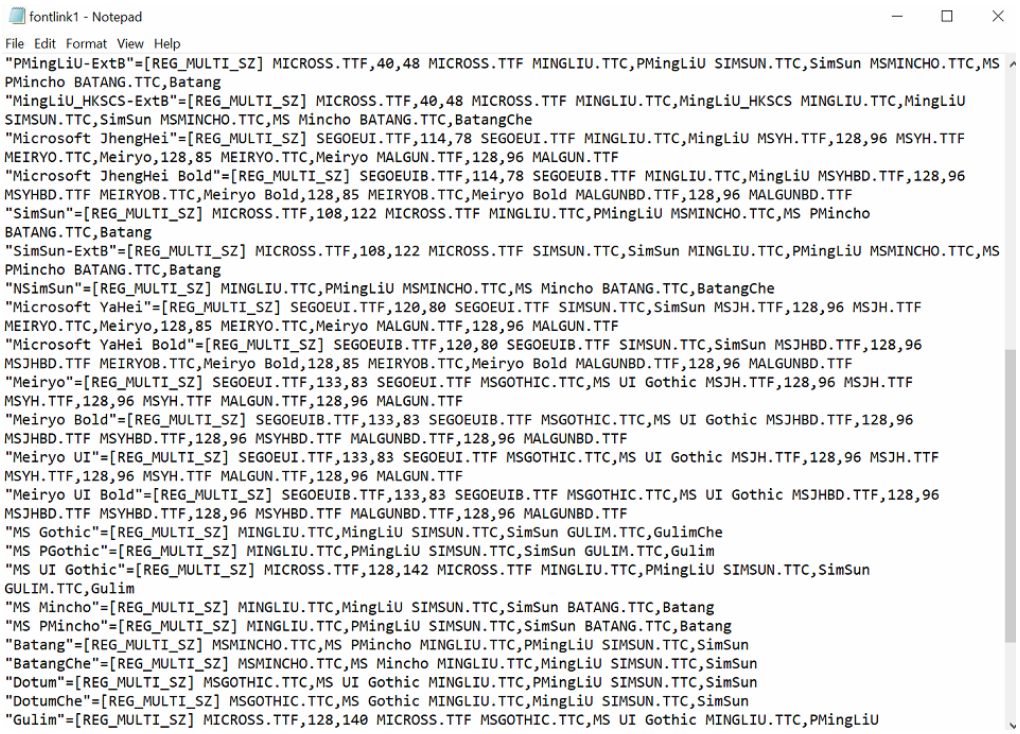
```
C:\Users\pshra\Desktop\SUNU\VB>RegToText.exe  C:\Users\pshra\Desktop\SUNU\VB\reg-fontl
ink.reg /o:C:\Users\pshra\Desktop\SUNU\VB\fontlink1.txt /e:ASCII
Selected encoding with ASCII
Reading file C:\Users\pshra\Desktop\SUNU\VB\reg-fontlink.reg
Valid windows registry header.
Writing chunk number (@ 20 lines each)
1
Processed entire file.
Success.

Wrote out 47 lines.
Processed 2 subkeys paths and 42 key/value pairs.
Runtime: 81 milliseconds

Input  file: C:\Users\pshra\Desktop\SUNU\VB\reg-fontlink.reg
Output file: C:\Users\pshra\Desktop\SUNU\VB\fontlink1.txt

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
This is unlicensed "demo" software and is provided "AS IS", WITHOUT WARRANTY OF
ANY KIND.

Read Full License Agreement use /l
OR pipe 'regtotext /l > RTTLic.txt' to read license in Notepad.

For a fully licensed version of this software, contact metadataconsult@gmail.com

This unlicensed “demo” version is provided for demonstration purposes only.
Unlicensed “demo” version is limited to read and translate a few lines. You can
use this software to showcase the product to others customers. You may not leave
the product with a customer after a demonstration has been completed.

NOTE: This unlicensed “demo” version will open a blog page on each run! Licensed
version will stop this action.
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
```

fontlink1 - Notepad

File Edit Format View Help

```
RegtoText Windows Registry Conversion Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink]
"FontLinkControl"=[REG_DWORD] 0
"FontLinkDefaultChar"=[REG_BINARY:<UTF16-LE,2-byte>] vvttuu

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink]
"MS PGothic MC"=[REG_MULTI_SZ] C:\Windows\ehome\WTVGOTHIC-S.ttc,Windows TV PGothic MINGLIU.TTC,PMingLiU
SIMSUN.TTC,SimSun GULIM.TTC,Gulim
"Segoe Media Center"=[REG_MULTI_SZ] tahoma.ttf MEIRYO.TTC,Meiryo,128,85 MSJH.TTF,128,96 mingliub.ttc,PMingLiU-ExtB
MSYH.TTF,128,96 simsunb.ttf C:\Windows\ehome\malgunmc.ttf,128,96 C:\Windows\ehome\WTVGOTHIC-S.ttc,Windows TV
PGothic
"Segoe Media Center Semibold"=[REG_MULTI_SZ] tahoma.ttf MEIRYO.TTC,Meiryo,128,85 MSJH.TTF,128,96
mingliub.ttc,PMingLiU-ExtB MSYH.TTF,128,96 simsunb.ttf C:\Windows\ehome\malgunmc.ttf,128,96 C:\Windows\ehome
\WTVGOTHIC-S.ttc,Windows TV PGothic
"Segoe Media Center Light"=[REG_MULTI_SZ] tahoma.ttf MEIRYO.TTC,Meiryo,128,85 MSJH.TTF,128,96
mingliub.ttc,PMingLiU-ExtB MSYH.TTF,128,96 simsunb.ttf C:\Windows\ehome\malgunmc.ttf,128,96 C:\Windows\ehome
\WTVGOTHIC-S.ttc,Windows TV PGothic
"Lucida Sans Unicode"=[REG_MULTI_SZ] MSGOTHIC.TTC,MS UI Gothic MINGLIU.TTC,PMingLiU SIMSUN.TTC,SimSun
GULIM.TTC,Gulim
"Microsoft Sans Serif"=[REG_MULTI_SZ] MSGOTHIC.TTC,MS UI Gothic MINGLIU.TTC,PMingLiU SIMSUN.TTC,SimSun
GULIM.TTC,Gulim
"Tahoma"=[REG_MULTI_SZ] MSGOTHIC.TTC,MS UI Gothic MINGLIU.TTC,PMingLiU SIMSUN.TTC,SimSun GULIM.TTC,Gulim
"Segoe UI"=[REG_MULTI_SZ] TAHOMA.TTF MEIRYO.TTC,Meiryo,128,85 MEIRYO.TTC,Meiryo MSGOTHIC.TTC,MS UI Gothic
MSJH.TTF,128,96 MSJH.TTF MSYH.TTF,128,96 MSYH.TTF MALGUN.TTF,128,96 MALGUN.TTF MINGLIU.TTC,PMingLiU
SIMSUN.TTC,SimSun GULIM.TTC,Gulim
"MingLiU"=[REG_MULTI_SZ] MICROSS.TTF,40,48 MICROSS.TTF SIMSUN.TTC,SimSun MSMINCHO.TTC,MS Mincho
BATANG.TTC,BatangChe
"PMingLiU"=[REG_MULTI_SZ] MICROSS.TTF,40,48 MICROSS.TTF SIMSUN.TTC,SimSun MSMINCHO.TTC,MS PMincho BATANG.TTC,Batang

"MingLiU_HKSCS"=[REG_MULTI_SZ] MICROSS.TTF,40,48 MICROSS.TTF MINGLIU.TTC,MingLiU SIMSUN.TTC,SimSun MSMINCHO.TTC,MS
Mincho BATANG.TTC,BatangChe
"MingLiU-ExtB"=[REG_MULTI_SZ] MICROSS.TTF,40,48 MICROSS.TTF MINGLIU.TTC,MingLiU SIMSUN.TTC,SimSun MSMINCHO.TTC,MS
Mincho BATANG.TTC,BatangChe
"PMingLiU-ExtB"=[REG_MULTI_SZ] MICROSS.TTF,40,48 MICROSS.TTF MINGLIU.TTC,PMingLiU SIMSUN.TTC,SimSun MSMINCHO.TTC,MS
PMincho BATANG.TTC,Batang
```

Mail



Windows registry rootkit abides by the instructions given in the registry files.