Malware Analysis Report [Sample2.exe]

Prepared by: Sameer Patil

Mentors: Amit Malik & Monnappa KA

[SecurityXploded Student Mentorship Programme]

General Information

- File name: sample2.exe
- MD5: 23c75249b1e30e332cdcb65c7aace588
- SHA-1: 828ab6e73dd8de65fb050b68d855cd3a4db594e5
- File Size: 105.8 KB
- First Submission on: 20-11-2011
- Identified as: Backdoor.Win32.Ginwui.a [Kaspersky]
  Backdoor.Win32.Ginwui.B [Comodo]
  Generic MultiDropper.b [McAfee]

Analysis Overview:

Sample2.exe being identified as Backdoor.Win32.Ginwui.a is a trojan that installs a backdoor and rootkit on impacted systems. It was originally dropped and executed by TrojanDropper:Win32/Starx.A.

Technical Analysis:

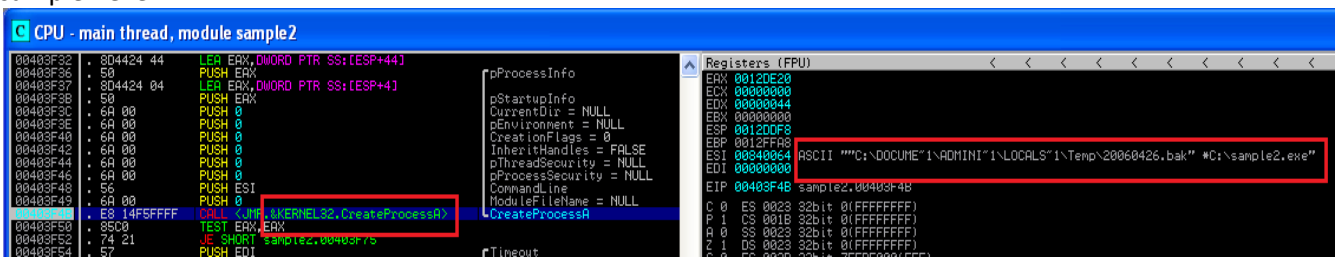
1. Backdoor:Win32/Ginwui.A begins its activities by copying itself to <temp> folder.

```
[Excerpt from CaptureBat analysis report]

process: created C:\WINDOWS\explorer.exe -> C:\sample2.exe
file: Write C:\sample2.exe -> C:\Documents and Settings\Administrator\Local Settings\Temp\20060426.bak
```

"20060426.bak" string can easily be found in the executable. Hence malware detection becomes very easy here. Static Analysis of the executable will identify it as a malware.

```
00404134  . 25 54 45 4D 5( ASCII "%TEMP%\20060426."
00404144  . 62 61 6B 00    ASCII "bak",0
00404148  . FFFFFFFF       DD FFFFFFFF
0040414C  . 01000000       DD 00000001
00404150  . 22 00          ASCII """,0
00404152    00             DB 00
```

2. 20060426.bak is executed with two command-line arguments. The first argument is the path to the copy, <*temp*>\20060426.bak; the second argument is the path to the original file sample2.exe.



3. 20060426.bak drops two DLLs in the system32 folder.

```
[Excerpt from CaptureBat analysis report]

file: Write C:\Documents and Settings\Administrator\Local Settings\Temp\20060426.bak ->
C:\WINDOWS\system32\zsyhide.dll
file: Write C:\Documents and Settings\Administrator\Local Settings\Temp\20060426.bak ->
C:\WINDOWS\system32\zsydll.dll
```

4. Adds "<SystemRoot>\zsydll.dll" in the AppInit_DLLs list. The AppInit DLLs are loaded by using the **LoadLibrary()** function during the **DLL_PROCESS_ATTACH** process of User32.dll.

```
[Excerpt from Regshot analysis report]

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs:
"C:\WINDOWS\system32\zsyhide.dll"
```

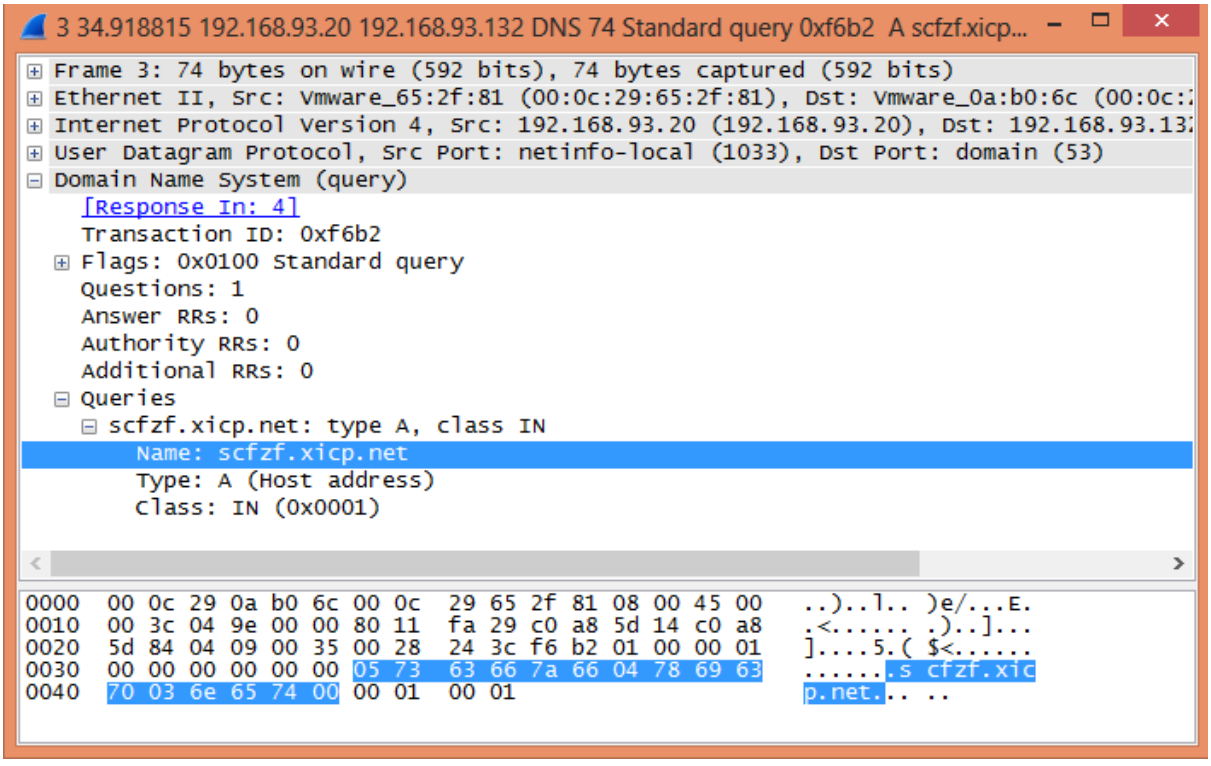
5. zsydll.dll is injected in the Winlogon process so that it executes each time system boots. It creates the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\zsydll.
The key also creates the following values:

```
[Excerpt from CaptureBat analysis report]

registry: SetValueKey C:\Documents and Settings\Administrator\Local Settings\Temp\20060426.bak -> HKLM\SOFTWARE\
Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\zsydll\DllName
registry: SetValueKey C:\Documents and Settings\Administrator\Local Settings\Temp\20060426.bak -> HKLM\SOFTWARE\
Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\zsydll\Shutdown
registry: SetValueKey C:\Documents and Settings\Administrator\Local Settings\Temp\20060426.bak -> HKLM\SOFTWARE\
Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\zsydll\Startup
registry: SetValueKey C:\Documents and Settings\Administrator\Local Settings\Temp\20060426.bak -> HKLM\SOFTWARE\
Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\zsydll\Asynchronous
registry: SetValueKey C:\Documents and Settings\Administrator\Local Settings\Temp\20060426.bak -> HKLM\SOFTWARE\
Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\zsydll\Impersonate
```

6. It injects *ZSYDLL.DLL* into the Internet Explorer process. This causes the Internet Explorer to crash.

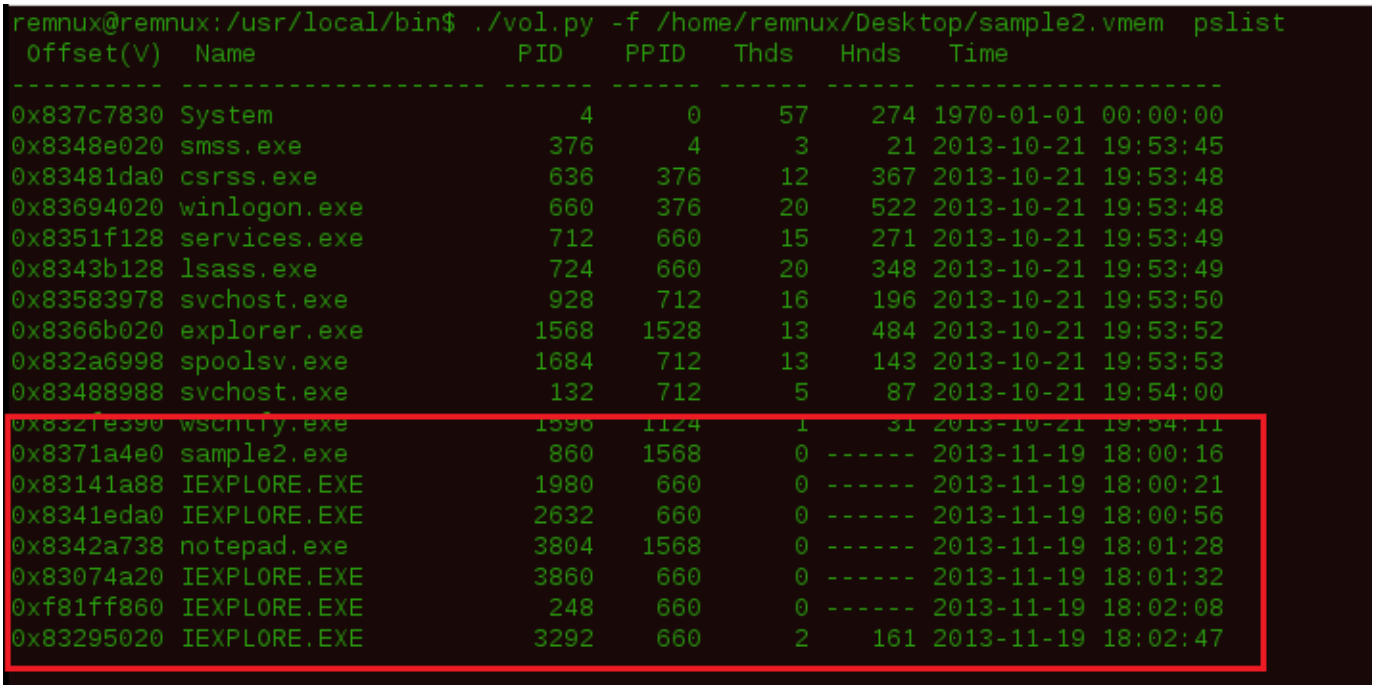
```
[Excerpt from CaptureBat analysis report]

registry: SetValueKey C:\Program Files\Internet Explorer\IEXPLORE.EXE -> HKU\.DEFAULT\Software\Microsoft\Windows
\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
registry: SetValueKey C:\Program Files\Internet Explorer\IEXPLORE.EXE -> HKU\.DEFAULT\Software\Microsoft\Windows
\CurrentVersion\Explorer\Shell Folders\Cache
registry: SetValueKey C:\Program Files\Internet Explorer\IEXPLORE.EXE -> HKU\.DEFAULT\Software\Microsoft\Windows
\CurrentVersion\Explorer\Shell Folders\Cookies
registry: SetValueKey C:\Program Files\Internet Explorer\IEXPLORE.EXE -> HKU\.DEFAULT\Software\Microsoft\Windows
\CurrentVersion\Explorer\Shell Folders\History
registry: SetValueKey C:\Program Files\Internet Explorer\IEXPLORE.EXE -> HKU\.DEFAULT\Software\Microsoft\Windows
\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
registry: SetValueKey C:\Program Files\Internet Explorer\IEXPLORE.EXE -> HKU\.DEFAULT\Software\Microsoft\Windows
\CurrentVersion\Internet Settings\ZoneMap\IntranetName
registry: SetValueKey C:\Program Files\Internet Explorer\IEXPLORE.EXE -> HKU\.DEFAULT\Software\Microsoft\Windows
\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
```

7. Contacts C&C server for control over the victim and sending information.



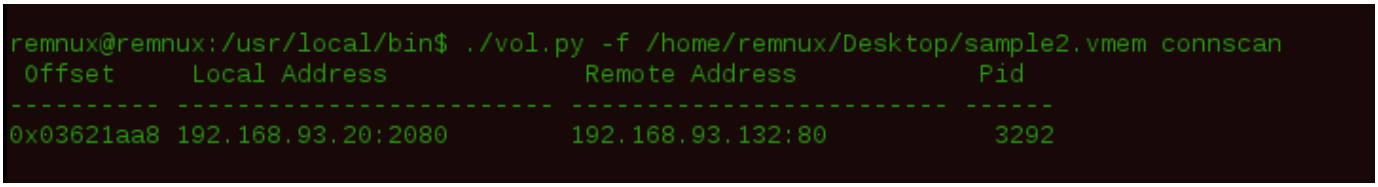
Memory Analysis using Volatility

1. List all the processes running after executing the sample.



```
remnux@remnux:/usr/local/bin$ ./vol.py -f /home/remnux/Desktop/sample2.vmem  pslist
 Offset(V)  Name                    PID    PPID   Thds   Hnds   Time
---------- -------------------- ------ ------ ------ ------ ------------------
0x837c7830 System                    4      0     57    274 1970-01-01 00:00:00
0x8348e020 smss.exe                376      4      3     21 2013-10-21 19:53:45
0x83481da0 csrss.exe               636    376     12    367 2013-10-21 19:53:48
0x83694020 winlogon.exe            660    376     20    522 2013-10-21 19:53:48
0x8351f128 services.exe            712    660     15    271 2013-10-21 19:53:49
0x8343b128 lsass.exe               724    660     20    348 2013-10-21 19:53:49
0x83583978 svchost.exe             928    712     16    196 2013-10-21 19:53:50
0x8366b020 explorer.exe           1568   1528     13    484 2013-10-21 19:53:52
0x832a6998 spoolsv.exe            1684    712     13    143 2013-10-21 19:53:53
0x83488988 svchost.exe             132    712      5     87 2013-10-21 19:54:00
0x832fe390 wscntfy.exe            1596   1124      1     31 2013-10-21 19:54:11
0x8371a4e0 sample2.exe             860   1568      0 ------ 2013-11-19 18:00:16
0x83141a88 IEXPLORE.EXE           1980    660      0 ------ 2013-11-19 18:00:21
0x8341eda0 IEXPLORE.EXE           2632    660      0 ------ 2013-11-19 18:00:56
0x8342a738 notepad.exe            3804   1568      0 ------ 2013-11-19 18:01:28
0x83074a20 IEXPLORE.EXE           3860    660      0 ------ 2013-11-19 18:01:32
0xf81ff860 IEXPLORE.EXE            248    660      0 ------ 2013-11-19 18:02:08
0x83295020 IEXPLORE.EXE           3292    660      2    161 2013-11-19 18:02:47
```

2. Check all the TCP connections established using connscan. The IEXPLORE.EXE process seems to have established a connection here.



```
remnux@remnux:/usr/local/bin$ ./vol.py -f /home/remnux/Desktop/sample2.vmem connscan
 Offset     Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ------
0x03621aa8 192.168.93.20:2080        192.168.93.132:80          3292
```

3. We previously saw that zsyhide.dll and zsydll.dll which were dropped by “20060426.bak” process are imported by the IEXPLORE.EXE process. Let’s confirm this once again. Hence this process is involved in malicious activities.

```
remnux@remnux:/usr/local/bin$ ./vol.py -f /home/remnux/Desktop/sample2.vmem dlllist -p 3292
************************************************************************
IEXPLORE.EXE pid:   3292
Command line : "C:\Program Files\Internet Explorer\IEXPLORE.EXE"
Service Pack 2

Base         Size         Path
0x00400000   0x019000     C:\Program Files\Internet Explorer\IEXPLORE.EXE
0x7c900000   0x0b0000     C:\WINDOWS\system32\ntdll.dll
0x7c800000   0x0f4000     C:\WINDOWS\system32\kernel32.dll
0x77c10000   0x058000     C:\WINDOWS\system32\msvcrt.dll
0x77d40000   0x090000     C:\WINDOWS\system32\USER32.dll
0x77f10000   0x046000     C:\WINDOWS\system32\GDI32.dll
0x77dd0000   0x09b000     C:\WINDOWS\system32\ADVAPI32.dll
0x77a80000   0x094000     C:\WINDOWS\system32\CRYPT32.dll
0x754d0000   0x080000     C:\WINDOWS\system32\CRYPTUI.dll
0x5b860000   0x054000     C:\WINDOWS\system32\NETAPI32.dll
0x771b0000   0x0a6000     C:\WINDOWS\system32\WININET.dll
0x00600000   0x008000     C:\WINDOWS\system32\zsyhide.dll
0x00740000   0x00e000     C:\WINDOWS\system32\zsydll.dll
0x71ad0000   0x009000     C:\WINDOWS\system32\wsock32.dll
```

4. We can also dump the DLLs at the memory addresses where they are located in memory.

```
remnux@remnux:/usr/local/bin$ ./vol.py -f /home/remnux/Desktop/sample2.vmem dlldump -p 3292 -b 0x00600000
-D /home/remnux/Desktop/
Dumping zsyhide.dll, Process: IEXPLORE.EXE, Base:   600000 output: module.3292.3295020.600000.dll

remnux@remnux:/usr/local/bin$ ./vol.py -f /home/remnux/Desktop/sample2.vmem dlldump -p 3292 -b 0x00740000
-D /home/remnux/Desktop/
Dumping zsydll.dll, Process: IEXPLORE.EXE, Base:   740000 output: module.3292.3295020.740000.dll
```

These DLLs definitely assist the Trojan in communicating with C&C servers and to monitor activities of the victims.