

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 40 5i 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.

CPU - main thread, module sample2

```
00403F32 . 804424 44 LEA EAX, DWORD PTR SS:[ESP+44]
00403F36 . 50 PUSH EAX
00403F37 . 804424 04 LEA EAX, DWORD PTR SS:[ESP+4]
00403F3B . 50 PUSH EAX
00403F3C . 6A 00 PUSH 0
00403F3E . 6A 00 PUSH 0
00403F40 . 6A 00 PUSH 0
00403F42 . 6A 00 PUSH 0
00403F44 . 6A 00 PUSH 0
00403F46 . 6A 00 PUSH 0
00403F48 . 56 PUSH ESI
00403F49 . 6A 00 PUSH 0
00403F50 . 85C0 TEST EAX, EAX
00403F52 . 74 21 JE SHORT sample2.00403F75
00403F54 . 57 PUSH EDI
```

Registers (FPU)

```
EAX 00120E20
ECX 00000000
EDX 00000044
EBX 00000000
ESP 00120DF8
EBP 0012FFA8
ESI 00840064 ASCII "%C:\DOCUMENTS\1\ADMINI\1\LOCALS\1\Temp\20060426.bak\" #C:\sample2.exe"
EDI 00000000
EIP 00403F48 sample2.00403F48
```

pProcessInfo

```
pStartupInfo
CurrentDir = NULL
pEnvironment = NULL
CreationFlags = 0
InheritHandles = FALSE
pThreadSecurity = NULL
pProcessSecurity = NULL
CommandLine
ModuleFileName = NULL
```

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
```

- 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
```

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

The screenshot shows a network traffic analysis window with the following details:

- Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
- Ethernet II, Src: vmware_65:2f:81 (00:0c:29:65:2f:81), Dst: vmware_0a:b0:6c (00:0c:29:0a:b0:6c)
- Internet Protocol Version 4, Src: 192.168.93.20 (192.168.93.20), Dst: 192.168.93.132 (192.168.93.132)
- User Datagram Protocol, Src Port: netinfo-local (1033), Dst Port: domain (53)
- Domain Name System (query)
 - [Response In: 4]
 - Transaction ID: 0xf6b2
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - sczfq.xicp.net: type A, class IN
 - Name: sczfq.xicp.net
 - Type: A (Host address)
 - Class: IN (0x0001)

Below the packet details, a hex dump shows the raw data of the query:

```

0000  00 0c 29 0a b0 6c 00 0c 29 65 2f 81 08 00 45 00  ..)..l.. )e/...E.
0010  00 3c 04 9e 00 00 80 11 fa 29 c0 a8 5d 14 c0 a8  .<..... )...]...
0020  5d 84 04 09 00 35 00 28 24 3c f6 b2 01 00 00 01  ]...5.( $<.....
0030  00 00 00 00 00 00 05 73 63 66 7a 66 04 78 69 63  .....s cfzf.xic
0040  70 03 6e 65 74 00 00 01 00 01                   p.net... ..
  
```

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 conncscan. The IEXPLORE.EXE process seems to have established a connection here.

```
remnux@remnux:/usr/local/bin$ ./vol.py -f /home/remnux/Desktop/sample2.vmem conncscan
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    0x000000     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.