Malware Analysis
Report created by: Matt (MTTGIT19)
Prepared for: Masters lab Course work – GitHub Version

Summary:

Name: Bot.exe
Nicknames: Backdoor, Freeload.
Analysis findings: **Malware/Spyware**

Behavior:

- Connects to outside network.
- Accesses browser information
- Reads computer name and windows account information.
- Changes Windows registry keys

This sample was first created April 04, 2016, according to Virustotal.com. The analysis shows this specific file named Bot.exe was created locally on May 02, 2017, and modified October 04, 2016.

MD5: 361C983B94B3E07A3B509F0B9B34CAD7
SHA256: 6BD51F44230010E4C435C63364F26188531908035000E747721732F9735C96C1

Environment: Windows 7 Professional, Service Pack 1. 32-bit OS.

Tools:

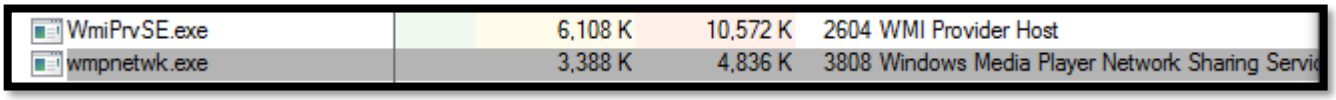
- IDA Pro Free v5.0
- QuickHash-Windows v2.8.0
- PEid v0.65
- Process Explorer v16.20
- Process Monitor v3.32
- Regshot v1.8.3
- Remnux
- WireShark 3.6.5

Evidence:

Dynamic analysis results:

Firstly, using Process Explorer analysts compared the processes running before and after executing Bot.exe. After running for several minutes, the Bot.exe file, an unsolicited Windows process starting called "wmpnetwk.exe" or Windows Media Player Network Sharing Service.

Bot	10/4/2016 8:28 PM	Application	330 KB



WmiPrvSE.exe	6,108 K	10,572 K	2604 WMI Provider Host
wmpnetwk.exe	3,388 K	4,836 K	3808 Windows Media Player Network Sharing Servic

To investigate further, analysts looked at the strings of Bot.exe to find several suspicious entries, seen below.

```
Windows Media Player Network Sharing Service CDS
System
IdleSecondsUntilSleep
WMPNetworkSvc
NT AUTHORITY\NetworkService
UNKNOWN_SERVICE
SYSTEM\CurrentControlSet\Services\
Software\Microsoft\MediaPlayer\Preferences\HME\
SharedLibraryPath
EnableDlnaTags
UPnPDeviceID
SOFTWARE\Microsoft\Windows Media Player NSS\3.0\Media Servers
@FirewallAPI.dll,-31252
SkipFirewallCheckOnUPnPAction
WakeOnMagicPacketEnabled
```

Initial evidence suggests that this executable appears to use Windows Media Player to call out through the system firewall. Several strings reference the firewall or skipping firewall checks, along with changes to Windows Media Player. To confirm these findings, Remnux with WireShark was used to monitor the victims network activity.

```
NBNS        92 Name query NB WIN-GH5N83N4HRV<1c>
NBNS        92 Name query NB WIN-GH5N83N4HRV<1c>
NBNS        92 Name query NB WIN-GH5N83N4HRV<1c>
NBNS        92 Name query NB DIGI-SERV.BE<00>
NBNS        92 Name query NB DIGI-SERV.BE<00>
```

Two malicious callouts were observed, including call outs to “DIGI-SERV.BE”, located in Germany according to HybridAnalysis.com (Hybrid Analysis, 2016). In addition, we also see the system name of the victim computer being broadcast via NBNS. NBNS stands for NetBIOS Name Service which runs on port 137 (WireShark, 2020). This is an indicator of compromise, demonstrating Bot.exe is acting as Spyware, broadcasting computer information to other networks.

Lastly, ProcMon and RegShot were used to compare Windows Registry keys, before and after executing the malware. Immediately noticeable was that Bot.Exe triggered “NOTEPAD.EXE” numerous times, to edit, delete and create Windows Registry Keys.

```
----------------------------------
Keys added:4
----------------------------------
HKLM\SOFTWARE\Microsoft\Tracing\Bot_RASAPI32
HKLM\SOFTWARE\Microsoft\Tracing\Bot_RASMANCS
HKU\S-1-5-21-1978952113-2449162814-3274240734-1000\Software\Classes\Local Sett
HKU\S-1-5-21-1978952113-2449162814-3274240734-1000_Classes\Local Settings\Soft

----------------------------------
values added:37
----------------------------------
HKLM\SOFTWARE\Microsoft\Tracing\Bot_RASAPI32\EnableFileTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\Bot_RASAPI32\EnableConsoleTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\Bot_RASAPI32\FileTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\Bot_RASAPI32\ConsoleTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\Bot_RASAPI32\MaxFileSize: 0x00100000
HKLM\SOFTWARE\Microsoft\Tracing\Bot_RASAPI32\FileDirectory: "%windir%\tracing"
HKLM\SOFTWARE\Microsoft\Tracing\Bot_RASMANCS\EnableFileTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\Bot_RASMANCS\EnableConsoleTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\Bot_RASMANCS\FileTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\Bot_RASMANCS\ConsoleTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\Bot_RASMANCS\MaxFileSize: 0x00100000
HKLM\SOFTWARE\Microsoft\Tracing\Bot_RASMANCS\FileDirectory: "%windir%\tracing"
```

```
11:50:...  NOTEPAD.EXE   2364  RegEnumKey
11:50:...  NOTEPAD.EXE   2364  RegEnumKey
11:50:...  NOTEPAD.EXE   2364  RegEnumKey
11:50:...  NOTEPAD.EXE   2364  RegEnumKey
11:50:...  NOTEPAD.EXE   2364  RegEnumKey
```

Bot.exe changes numerous Windows registry values; buffer overflow exploits are also seen during this process.

Bot.exe	4076	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{E29...	REPARSE	Desired Access
Bot.exe	4076	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{E29AC...	NAME NOT FOUND	Desired Access
Bot.exe	4076	RegCreateKey	HKCU\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections	SUCCESS	Desired Access
Bot.exe	4076	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connection...	BUFFER OVERFLOW	Length: 144
Bot.exe	4076	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connection...	BUFFER OVERFLOW	Length: 144

Many of the value's state "Bot_RASMANCS" or "Bot_RASAPI32" which are Remote Access API's (Process Library, 2022). These API's may not always be malicious, but in this use case they are likely being used by Bot.exe to make a persistent connection with outside networks.

Looking at the list of imports inside IDA Pro, we can see strings effecting KERNEL32, ADVAPI32, IPHLPAPI, USER32, SHELL32, SHLWAPI, WINNET and WS2_32. Several names begin to emerge that demonstrate a pattern, confirming previous evidence seen earlier. Below we can see that Bot.exe utilizes HTTP requests to try and establish a connection to the internet.

004371...		InternetSetOptionA	WININET
004371...		InternetCloseHandle	WININET
004371...		HttpQueryInfoA	WININET
004371...		InternetConnectA	WININET
004371E0		InternetQueryDataAvailable	WININET
004371E4		InternetReadFile	WININET
004371E8		HttpOpenRequestA	WININET
004371...		HttpSendRequestA	WININET
004371F0		InternetOpenA	WININET
004371F8	12	inet_ntoa	WS2_32

<u>Static analysis results:</u>

Using IDA Pro, we can also analyze the following binaries to paint help paint a basic flow of the programs code execution.

- **0x401d10** – Function doubles specific byte values inside variables 160, 144, 140, 124, 120 and others related to buffer length. Possible buffer overflow exploit as this function appears first and is referenced later.

```
dwBufferLength  = dword ptr -11Ch
Buffer          = dword ptr -118h
var_10          = dword ptr -10h
```

- **0x401f10** – Similar format as above but now references number of bytes read, buffer length, and number of bytes available. Likely analyzing buffer status for exploit.

```
dwNumberOfBytesRead= dword ptr -18h
dwBufferLength  = dword ptr -14h
dwNumberOfBytesAvailable= dword ptr -10h
```

- **0x405a10** – Calls internet connection after using localhost information, including username, server port, and server name.

```
push    0                   ; lpszPassword
mov     ecx, offset aLocalhost ; "localhost"
cmovnz  ecx, eax
movzx   eax, word ptr [esi+12h]
push    0                   ; lpszUserName
push    eax                 ; nServerPort
push    ecx                 ; lpszServerName
push    dword ptr [esi] ; hInternet
call    ds:InternetConnectA
mov     [esi+4], eax
```

- **0x4060c0** – This function copies information from memory to new location. Evidenced by numerous mov and esi statements.

```
mov     dword ptr [esi+0ECh], 0
mov     dword ptr [esi+0F0h], 0
mov     dword ptr [esi+0F4h], 0
```

- **0x406630** – This function sets up the remote API for command and control.

```
push    offset a?controllerApi ; "?controller=api&action=commands&id="
```

- **0x407d40** – Sets a large number of variables and arguments.

```
var_64          = dword ptr -64h
var_4C          = dword ptr -4Ch
var_48          = dword ptr -48h
var_44          = dword ptr -44h
var_40          = dword ptr -40h
```

- **0x4080e0** – Sets more variables and imports hLib Module. hLib is a program library for hierarchical matrices.

```
var_FC          = dword ptr -0FCh
hLibModule      = dword ptr -0F8h
var_E8          = dword ptr -0E8h
var_DC          = dword ptr -0DCh
```

- **0x409690** – This function establishes a Yandex API gateway with a user profile. Note: Yandex is a Russian technology company (Yandex, 2022).

```
push    offset aYandex_service ; "\\yandex_service"
sub     esp, 18h          ; int
mov     ecx, esp
push    0Fh               ; int
mov     dword ptr [ecx+14h], 0Fh
mov     dword ptr [ecx+10h], 0
push    offset Name       ; "ALLUSERSPROFILE"
```

While analyzing the assembly in IDA Pro, additional evidence suggests this malware originated from Russia. Bot.exe was found to read languages from all over the world including English, Spanish, German, and Chinese. However, the Russian language was absent, to confirm this, text searches were used, shown below.

Occurences of: russia

Address	Instruction

Occurences of: chinese

Address	Instruction
.rdata:0043CAA0	dd offset aChinese ; "chinese"
.rdata:0043CAAC	dd offset aChineseHongkon ; "chinese-hongkong"
.rdata:0043CAB8	dd offset aChineseSimplif ; "chinese-simplified"
.rdata:0043CAC4	dd offset aChineseSingapo ; "chinese-singapore"
.rdata:0043CAD0	dd offset aChineseTraditi ; "chinese-traditional"

Occurences of: english

Address	Instruction
.rdata:0043CA4C	dd offset aAmericanEnglis ; "american english"
.rdata:0043CA58	dd offset aAmericanEngl_0 ; "american-english"
.rdata:0043CAE8	dd offset aEnglishAmerica ; "english-american"
.rdata:0043CAF4	dd offset aEnglishAus ; "english-aus"
.rdata:0043CB00	dd offset aEnglishBelize ; "english-belize"
.rdata:0043CB0C	dd offset aEnglishCan ; "english-can"
.rdata:0043CB18	dd offset aEnglishCaribbe ; "english-caribbean"
.rdata:0043CB24	dd offset aEnglishIre ; "english-ire"

The absence of the Russian language suggests that this malware is designed to work with Windows computers with virtually every language, except Russian.

References

(n.d.).

Hybrid Analysis. (2016, November 18). *Bot.exe*. Retrieved from Hybrid Analysis: https://www.hybrid-analysis.com/sample/6bd51f44230010e4c435c63364f26188531908035000e747721732f9735c96c1/582f2842aac2ed247c3e991d

Process Library. (2022). *Rasapi32.dll*. Retrieved from Process Library: https://www.processlibrary.com/en/directory/files/rasapi32/24102/

Sikorski, M., & Honig, A. (2012). *Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software.* No Starch Press.

Virustotal. (2022, July 09). *Bot.exe*. Retrieved from Virustotal: https://www.virustotal.com/gui/file/6bd51f44230010e4c435c63364f26188531908035000e747721732f9735c96c1/behavior

WireShark. (2020, August 11). *NetBIOS Name Service (NBNS)*. Retrieved from WireShark: https://wiki.wireshark.org/NetBIOS/NBNS

Yandex. (2022). *About*. Retrieved from Yandex: https://yandex.com/company/general_info/yandex_today