

Tan Ton

CS 373

Malware Analysis Report

Lab 1

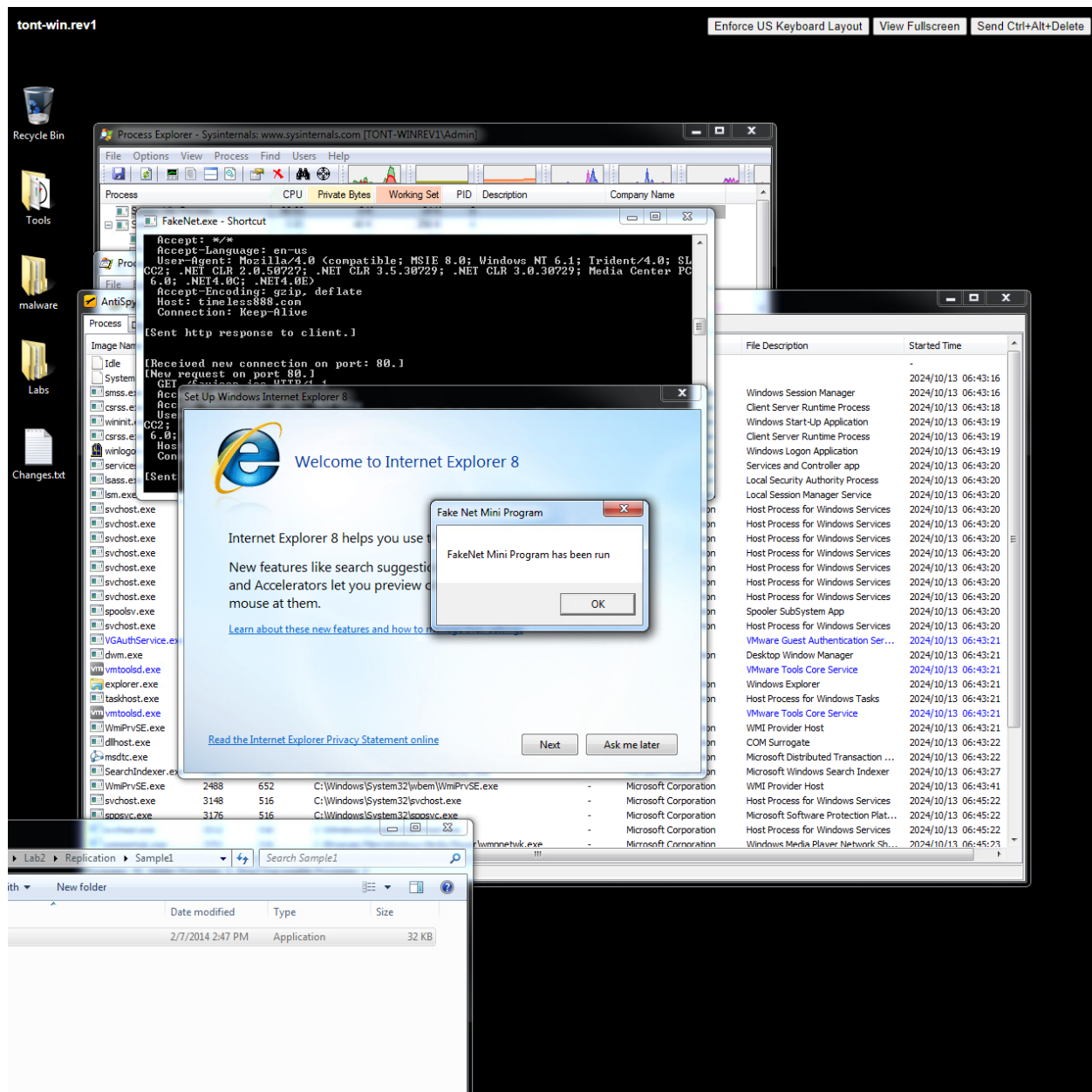
I follow the step that provided by professor to turn on vSphere VM using the win.rev1. After that, I got a snapshot from the VM that helped me revert to the original state before running Evil.exe, which later on will help me in writing this report.

After successfully turn on vSphere VM, I then do the following step

- Turn on Flypaper
- Turn on Fake net
- Turn on Process Monitor
- Turn on Process Explorer
- Turn on Anti spy
- Rename the file to evil.exe
- Double click on evil.exe

Note: If starting above tool before changing the file name to evil.exe, the VM easy to get “Not Responding”, which make me revert to original state multiple times to change the file name.

In



Picture 1

After starting evil.exe, I noticed a notification that told me to setup Internet Explorer 8, which gave me a question on why it starts up like this.

I then check on Fakenet.exe

Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
6:44:3...	FakeNet.exe	3136	WriteFile	C:\Users\Admin\Desktop\Tools\Faken...	SUCCESS	Offset: 107,702, Le...
6:44:3...	evil.exe	3420	TCP Receive	tort-winrev1.49158 -> tort-winrev1.htt...	SUCCESS	Length: 1024, seq...
6:44:3...	FakeNet.exe	3136	TCP Send	tort-winrev1.htt... -> tort-winrev1.49158	SUCCESS	Length: 1024, starti...
6:44:3...	FakeNet.exe	3136	WriteFile	C:\Users\Admin\Desktop\Tools\Faken...	SUCCESS	Offset: 108,726, Le...
6:44:3...	evil.exe	3420	WriteFile	C:\Users\Admin\AppData\Local\Micros...	SUCCESS	Offset: 66,560, Len...
6:44:3...	FakeNet.exe	3136	WriteFile	C:\Users\Admin\Desktop\Tools\Faken...	SUCCESS	Offset: 108,742, Le...
6:44:3...	evil.exe	3420	WriteFile	C:\Users\Admin\AppData\Local\Micros...	SUCCESS	Offset: 67,534, Len...
6:44:3...	FakeNet.exe	3136	WriteFile	C:\Users\Admin\Desktop\Tools\Faken...	SUCCESS	Offset: 108,762, Le...
6:44:3...	FakeNet.exe	3136	WriteFile	C:\Users\Admin\Desktop\Tools\Faken...	SUCCESS	Offset: 108,782, Le...
6:44:3...	evil.exe	3420	UDP Send	tort-winrev1.61314 -> tort-winrev1.61314	SUCCESS	Length: 1, sequen...
6:44:3...	evil.exe	3420	TCP Receive	tort-winrev1.49158 -> tort-winrev1.htt...	SUCCESS	Length: 1024, seq...
6:44:3...	evil.exe	3420	ReadFile	C:\Users\Admin\AppData\Local\Micros...	SUCCESS	Offset: 66,560, Len...
6:44:3...	evil.exe	3420	UDP Receive	tort-winrev1.61314 -> tort-winrev1.61314	SUCCESS	Length: 1, sequen...
6:44:3...	evil.exe	3420	ReadFile	C:\Users\Admin\AppData\Local\Micros...	SUCCESS	Offset: 68,608, Len...
6:44:3...	FakeNet.exe	3136	TCP Send	tort-winrev1.htt... -> tort-winrev1.49158	SUCCESS	Length: 1024, starti...
6:44:3...	FakeNet.exe	3136	WriteFile	C:\Users\Admin\Desktop\Tools\Faken...	SUCCESS	Offset: 109,806, Le...
6:44:3...	evil.exe	3420	WriteFile	C:\ntids\lainter.gif	SUCCESS	Offset: 66,560, Len...
6:44:3...	FakeNet.exe	3136	WriteFile	C:\Users\Admin\Desktop\Tools\Faken...	SUCCESS	Offset: 109,822, Le...
6:44:3...	FakeNet.exe	3136	WriteFile	C:\Users\Admin\Desktop\Tools\Faken...	SUCCESS	Offset: 109,842, Le...
6:44:3...	FakeNet.exe	3136	WriteFile	C:\Users\Admin\Desktop\Tools\Faken...	SUCCESS	Offset: 109,862, Le...
6:44:3...	evil.exe	3420	TCP Receive	tort-winrev1.49158 -> tort-winrev1.htt...	SUCCESS	Length: 1024, seq...
6:44:3...	FakeNet.exe	3136	TCP Send	tort-winrev1.htt... -> tort-winrev1.49158	SUCCESS	Length: 1024, starti...
6:44:3...	FakeNet.exe	3136	WriteFile	C:\Users\Admin\Desktop\Tools\Faken...	SUCCESS	Offset: 110,886, Le...
6:44:3...	FakeNet.exe	3136	WriteFile	C:\Users\Admin\Desktop\Tools\Faken...	SUCCESS	Offset: 110,902, Le...
6:44:3...	FakeNet.exe	3136	WriteFile	C:\Users\Admin\Desktop\Tools\Faken...	SUCCESS	Offset: 110,922, Le...
6:44:3...	FakeNet.exe	3136	WriteFile	C:\Users\Admin\Desktop\Tools\Faken...	SUCCESS	Offset: 110,942, Le...
6:44:3...	evil.exe	3420	TCP Receive	tort-winrev1.49158 -> tort-winrev1.htt...	SUCCESS	Length: 1024, seq...
6:44:3...	FakeNet.exe	3136	TCP Send	tort-winrev1.htt... -> tort-winrev1.49158	SUCCESS	Length: 1024, starti...
6:44:3...	FakeNet.exe	3136	WriteFile	C:\Users\Admin\Desktop\Tools\Faken...	SUCCESS	Offset: 111,966, Le...
6:44:3...	FakeNet.exe	3136	WriteFile	C:\Users\Admin\Desktop\Tools\Faken...	SUCCESS	Offset: 111,982, Le...
6:44:3...	FakeNet.exe	3136	WriteFile	C:\Users\Admin\Desktop\Tools\Faken...	SUCCESS	Offset: 112,002, Le...
6:44:3...	FakeNet.exe	3136	WriteFile	C:\Users\Admin\Desktop\Tools\Faken...	SUCCESS	Offset: 112,022, Le...
6:44:3...	evil.exe	3420	WriteFile	C:\Users\Admin\AppData\Local\Micros...	SUCCESS	Offset: 68,608, Len...
6:44:3...	evil.exe	3420	TCP Receive	tort-winrev1.49158 -> tort-winrev1.htt...	SUCCESS	Length: 1024, seq...
6:44:3...	evil.exe	3420	WriteFile	C:\Users\Admin\AppData\Local\Micros...	SUCCESS	Offset: 70,656, Len...
6:44:3...	FakeNet.exe	3136	TCP Send	tort-winrev1.htt... -> tort-winrev1.49158	SUCCESS	Length: 1024, starti...
6:44:3...	FakeNet.exe	3136	WriteFile	C:\Users\Admin\Desktop\Tools\Faken...	SUCCESS	Offset: 113,046, Le...

Showing 274,162 of 499,136 events (54%) Backed by virtual memory

Figure 3

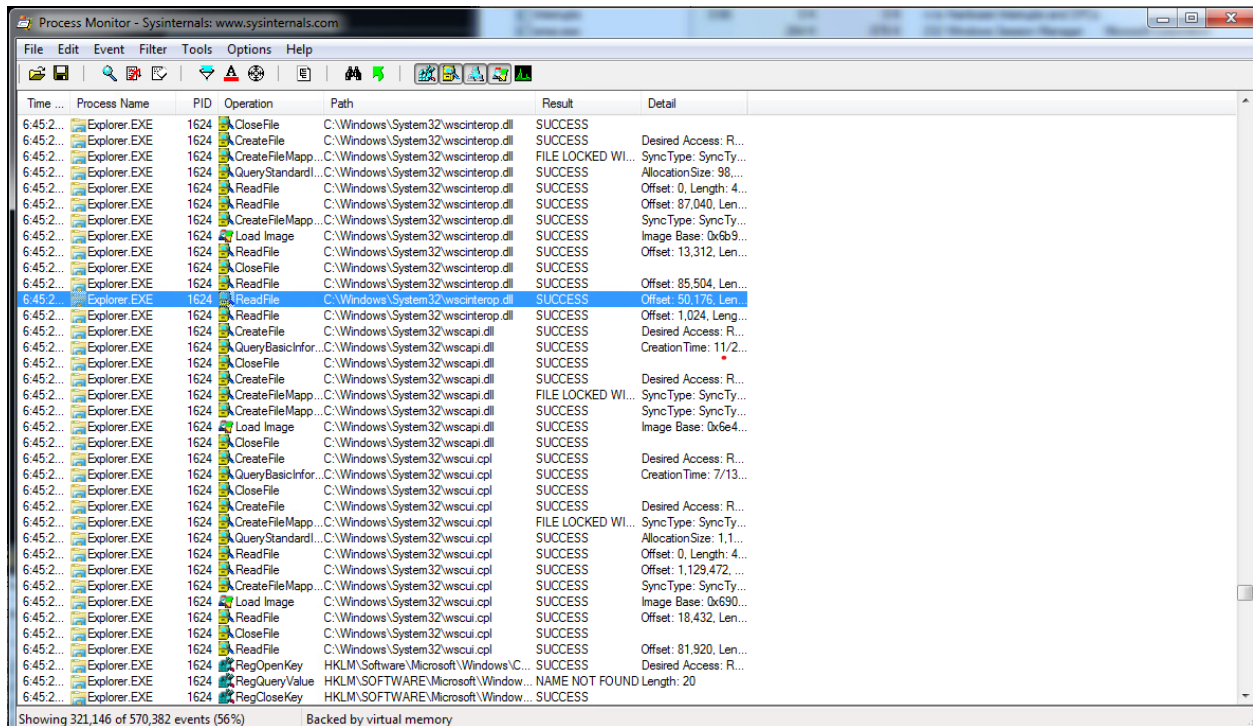
Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
6:44:4...	EXPLORE.EXE	3708	CloseFile	C:\Users\Admin\Favorites\Links	SUCCESS	
6:44:4...	EXPLORE.EXE	3708	RegOpenKey	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Desired Access: R...
6:44:4...	EXPLORE.EXE	3708	RegCloseKey	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	
6:44:4...	EXPLORE.EXE	3708	RegQueryValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Query: Cached, Su...
6:44:4...	EXPLORE.EXE	3708	RegEnumKey	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Index: 0, Name: 0
6:44:4...	EXPLORE.EXE	3708	RegEnumKey	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Index: 1, Name: 1
6:44:4...	EXPLORE.EXE	3708	RegQueryValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_SZ, Le...
6:44:4...	EXPLORE.EXE	3708	RegQueryValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_DWORD...
6:44:4...	EXPLORE.EXE	3708	RegQueryValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_SZ, Le...
6:44:4...	EXPLORE.EXE	3708	RegQueryValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_DWORD...
6:44:4...	EXPLORE.EXE	3708	RegCreateKey	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Desired Access: W...
6:44:4...	EXPLORE.EXE	3708	RegCloseKey	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	
6:44:4...	EXPLORE.EXE	3708	RegSetValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_SZ, Le...
6:44:4...	EXPLORE.EXE	3708	RegSetValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_SZ, Le...
6:44:4...	EXPLORE.EXE	3708	RegSetValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_SZ, Le...
6:44:4...	EXPLORE.EXE	3708	RegQueryValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_SZ, Le...
6:44:4...	EXPLORE.EXE	3708	RegSetValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_SZ, Le...
6:44:4...	EXPLORE.EXE	3708	RegQueryValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_DWORD...
6:44:4...	EXPLORE.EXE	3708	RegDeleteValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	
6:44:4...	EXPLORE.EXE	3708	RegQueryValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_DWORD...
6:44:4...	EXPLORE.EXE	3708	RegSetValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_DWORD...
6:44:4...	EXPLORE.EXE	3708	RegQueryValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_DWORD...
6:44:4...	EXPLORE.EXE	3708	RegCreateKey	HKLM\SOFTWARE\Microsoft\Internet ...	SUCCESS	Desired Access: W...
6:44:4...	EXPLORE.EXE	3708	RegCloseKey	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	
6:44:4...	EXPLORE.EXE	3708	RegSetValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_SZ, Le...
6:44:4...	EXPLORE.EXE	3708	RegSetValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_SZ, Le...
6:44:4...	EXPLORE.EXE	3708	RegSetValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_SZ, Le...
6:44:4...	EXPLORE.EXE	3708	RegQueryValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_SZ, Le...
6:44:4...	EXPLORE.EXE	3708	RegQueryValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_SZ, Le...
6:44:4...	EXPLORE.EXE	3708	RegDeleteValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	
6:44:4...	EXPLORE.EXE	3708	RegQueryValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_DWORD...
6:44:4...	EXPLORE.EXE	3708	RegSetValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_DWORD...
6:44:4...	EXPLORE.EXE	3708	RegQueryValue	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	Type: REG_DWORD...
6:44:4...	EXPLORE.EXE	3708	RegOpenKey	HKCU\Software\Microsoft\Internet Exp...	SUCCESS	NAME NOT FOUND Desired Access: R...

Showing 302,563 of 539,389 events (56%) Backed by virtual memory

Figure 4

Figure 4 is showing IEXPLORER.EXE is running in the background, which could be a fake copy from Explore.EXE from Figure 5



The screenshot shows the Process Monitor application window with a list of events for Explorer.EXE. The events are filtered to show only those for the process name 'Explorer.EXE'. The table below represents the data shown in the screenshot.

Time ...	Process Name	PID	Operation	Path	Result	Detail
6:45:2...	Explorer.EXE	1624	CloseFile	C:\Windows\System32\wsinterop.dll	SUCCESS	
6:45:2...	Explorer.EXE	1624	CreateFile	C:\Windows\System32\wsinterop.dll	SUCCESS	Desired Access: R...
6:45:2...	Explorer.EXE	1624	CreateFileMap...	C:\Windows\System32\wsinterop.dll	FILE LOCKED WI...	SyncType: SyncTy...
6:45:2...	Explorer.EXE	1624	QueryStandard...	C:\Windows\System32\wsinterop.dll	SUCCESS	AllocationSize: 98...
6:45:2...	Explorer.EXE	1624	ReadFile	C:\Windows\System32\wsinterop.dll	SUCCESS	Offset: 0, Length: 4...
6:45:2...	Explorer.EXE	1624	ReadFile	C:\Windows\System32\wsinterop.dll	SUCCESS	Offset: 87,040, Len...
6:45:2...	Explorer.EXE	1624	CreateFileMap...	C:\Windows\System32\wsinterop.dll	SUCCESS	SyncType: SyncTy...
6:45:2...	Explorer.EXE	1624	Load Image	C:\Windows\System32\wsinterop.dll	SUCCESS	Image Base: 0x6b9...
6:45:2...	Explorer.EXE	1624	ReadFile	C:\Windows\System32\wsinterop.dll	SUCCESS	Offset: 13,312, Len...
6:45:2...	Explorer.EXE	1624	CloseFile	C:\Windows\System32\wsinterop.dll	SUCCESS	
6:45:2...	Explorer.EXE	1624	ReadFile	C:\Windows\System32\wsinterop.dll	SUCCESS	Offset: 85,504, Len...
6:45:2...	Explorer.EXE	1624	ReadFile	C:\Windows\System32\wsinterop.dll	SUCCESS	Offset: 50,176, Len...
6:45:2...	Explorer.EXE	1624	ReadFile	C:\Windows\System32\wsinterop.dll	SUCCESS	Offset: 1,024, Leng...
6:45:2...	Explorer.EXE	1624	CreateFile	C:\Windows\System32\wsapi.dll	SUCCESS	Desired Access: R...
6:45:2...	Explorer.EXE	1624	QueryBasicInfor...	C:\Windows\System32\wsapi.dll	SUCCESS	CreationTime: 11/2...
6:45:2...	Explorer.EXE	1624	CloseFile	C:\Windows\System32\wsapi.dll	SUCCESS	
6:45:2...	Explorer.EXE	1624	CreateFile	C:\Windows\System32\wsapi.dll	SUCCESS	Desired Access: R...
6:45:2...	Explorer.EXE	1624	CreateFileMap...	C:\Windows\System32\wsapi.dll	FILE LOCKED WI...	SyncType: SyncTy...
6:45:2...	Explorer.EXE	1624	CreateFileMap...	C:\Windows\System32\wsapi.dll	SUCCESS	SyncType: SyncTy...
6:45:2...	Explorer.EXE	1624	Load Image	C:\Windows\System32\wsapi.dll	SUCCESS	Image Base: 0x6e4...
6:45:2...	Explorer.EXE	1624	CloseFile	C:\Windows\System32\wsapi.dll	SUCCESS	
6:45:2...	Explorer.EXE	1624	CreateFile	C:\Windows\System32\wsapi.dll	SUCCESS	Desired Access: R...
6:45:2...	Explorer.EXE	1624	QueryBasicInfor...	C:\Windows\System32\wsapi.dll	SUCCESS	CreationTime: 7/13...
6:45:2...	Explorer.EXE	1624	CloseFile	C:\Windows\System32\wsapi.dll	SUCCESS	
6:45:2...	Explorer.EXE	1624	CreateFile	C:\Windows\System32\wsapi.dll	SUCCESS	Desired Access: R...
6:45:2...	Explorer.EXE	1624	CreateFileMap...	C:\Windows\System32\wsapi.dll	FILE LOCKED WI...	SyncType: SyncTy...
6:45:2...	Explorer.EXE	1624	QueryStandard...	C:\Windows\System32\wsapi.dll	SUCCESS	AllocationSize: 1,1...
6:45:2...	Explorer.EXE	1624	ReadFile	C:\Windows\System32\wsapi.dll	SUCCESS	Offset: 0, Length: 4...
6:45:2...	Explorer.EXE	1624	ReadFile	C:\Windows\System32\wsapi.dll	SUCCESS	Offset: 1,129,472...
6:45:2...	Explorer.EXE	1624	CreateFileMap...	C:\Windows\System32\wsapi.dll	SUCCESS	SyncType: SyncTy...
6:45:2...	Explorer.EXE	1624	Load Image	C:\Windows\System32\wsapi.dll	SUCCESS	Image Base: 0x690...
6:45:2...	Explorer.EXE	1624	CloseFile	C:\Windows\System32\wsapi.dll	SUCCESS	Offset: 18,432, Len...
6:45:2...	Explorer.EXE	1624	ReadFile	C:\Windows\System32\wsapi.dll	SUCCESS	Offset: 81,920, Len...
6:45:2...	Explorer.EXE	1624	RegOpenKey	HKLM\Software\Microsoft\Windows\...	SUCCESS	Desired Access: R...
6:45:2...	Explorer.EXE	1624	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 20
6:45:2...	Explorer.EXE	1624	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	

Showing 321,146 of 570,382 events (56%) Backed by virtual memory

Figure 5

I later investigate the file and found a temporary internet file that contain the following files after running evil.exe

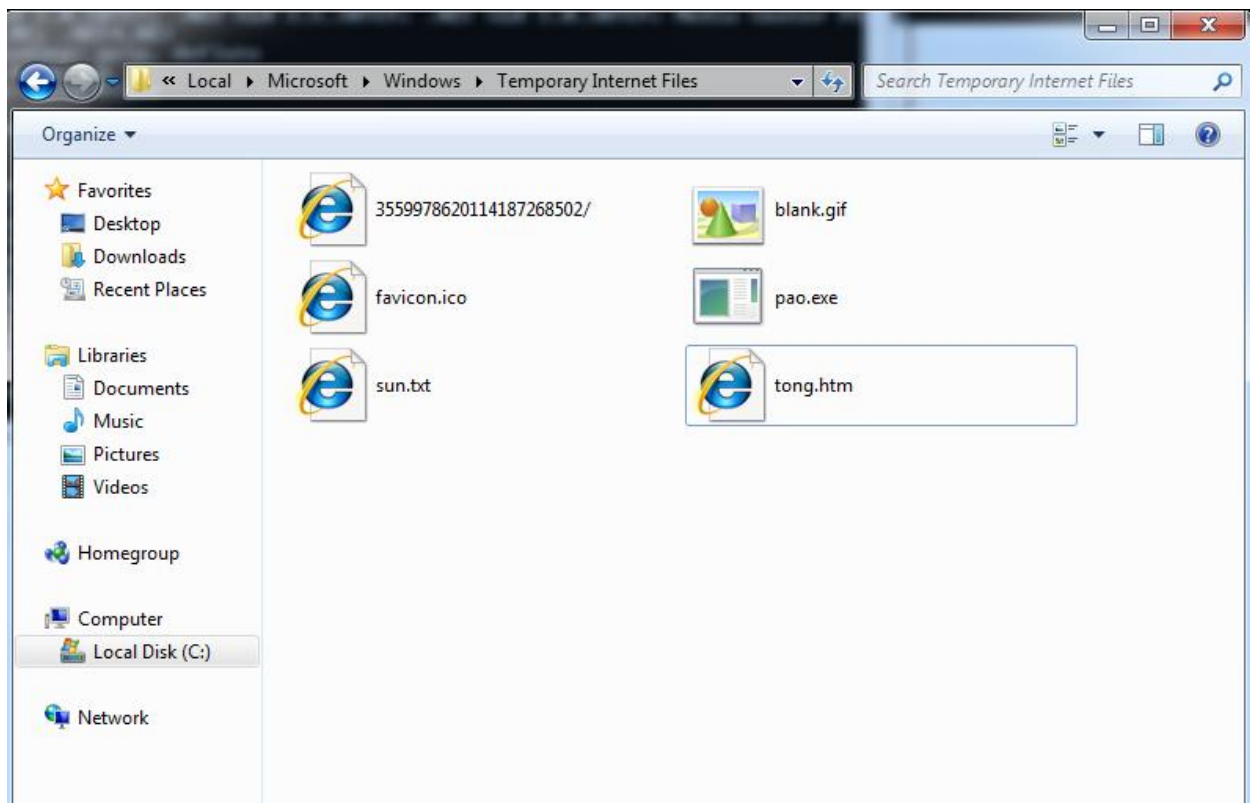


Figure 6

Pao.exe is a file that got downloaded from hisunpharm.com after executing evil.exe. The file could have been a second step to downloading another file, which is likely to be funbots.bat.

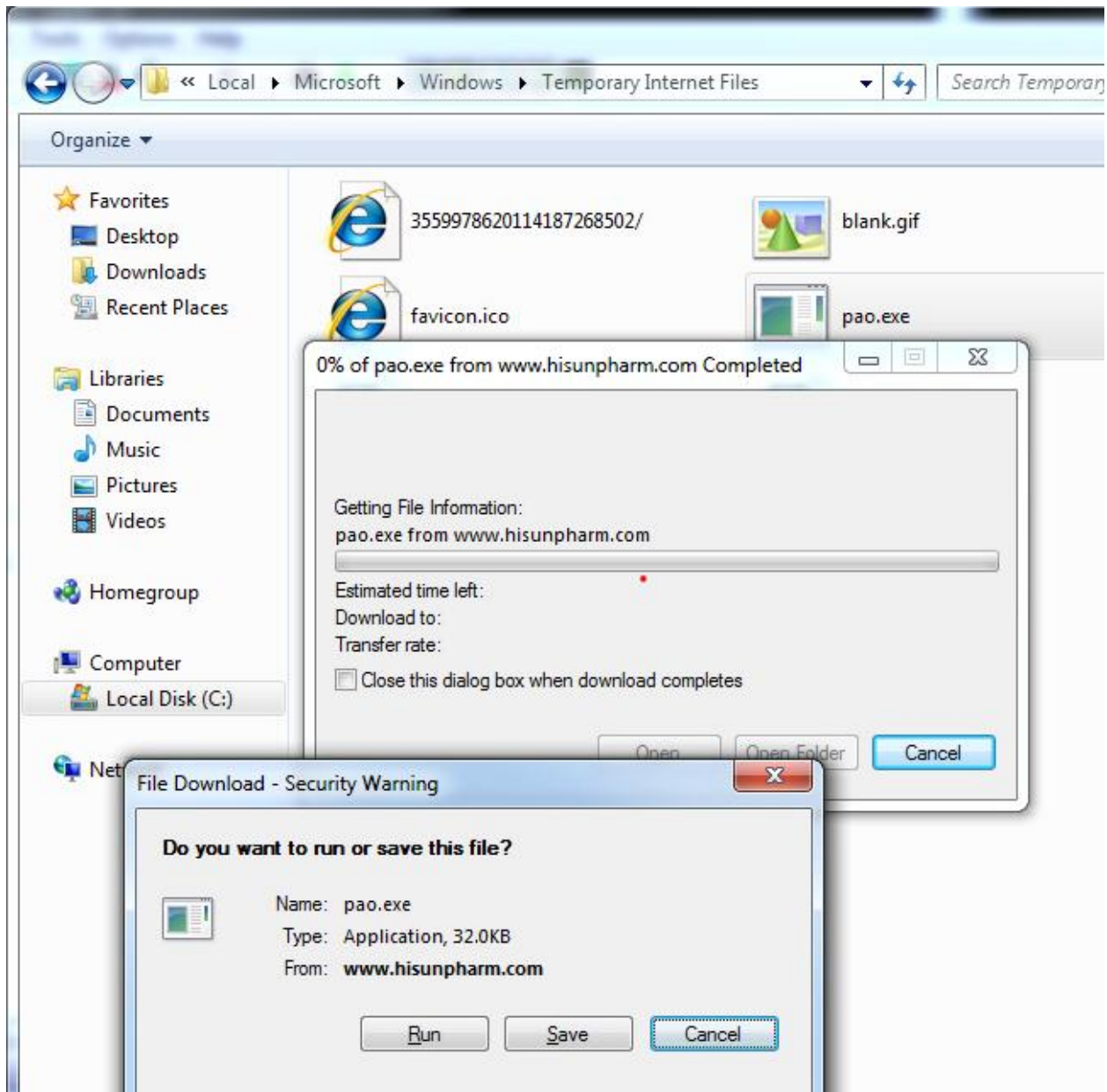


Figure 7

After running funbots.bat, there is a cmd popup saying about scheduled task was successfully deleted but, in the end, it said Access is Denied and The Requested service has already been started. Which means it could have been scheduled to run on some time when user use their computer and will keep running if user perform a particular action.

I believe the file funbots.bat is a script that helps attackers (evil.exe) hide their track by removing those scheduled tasks that they have.

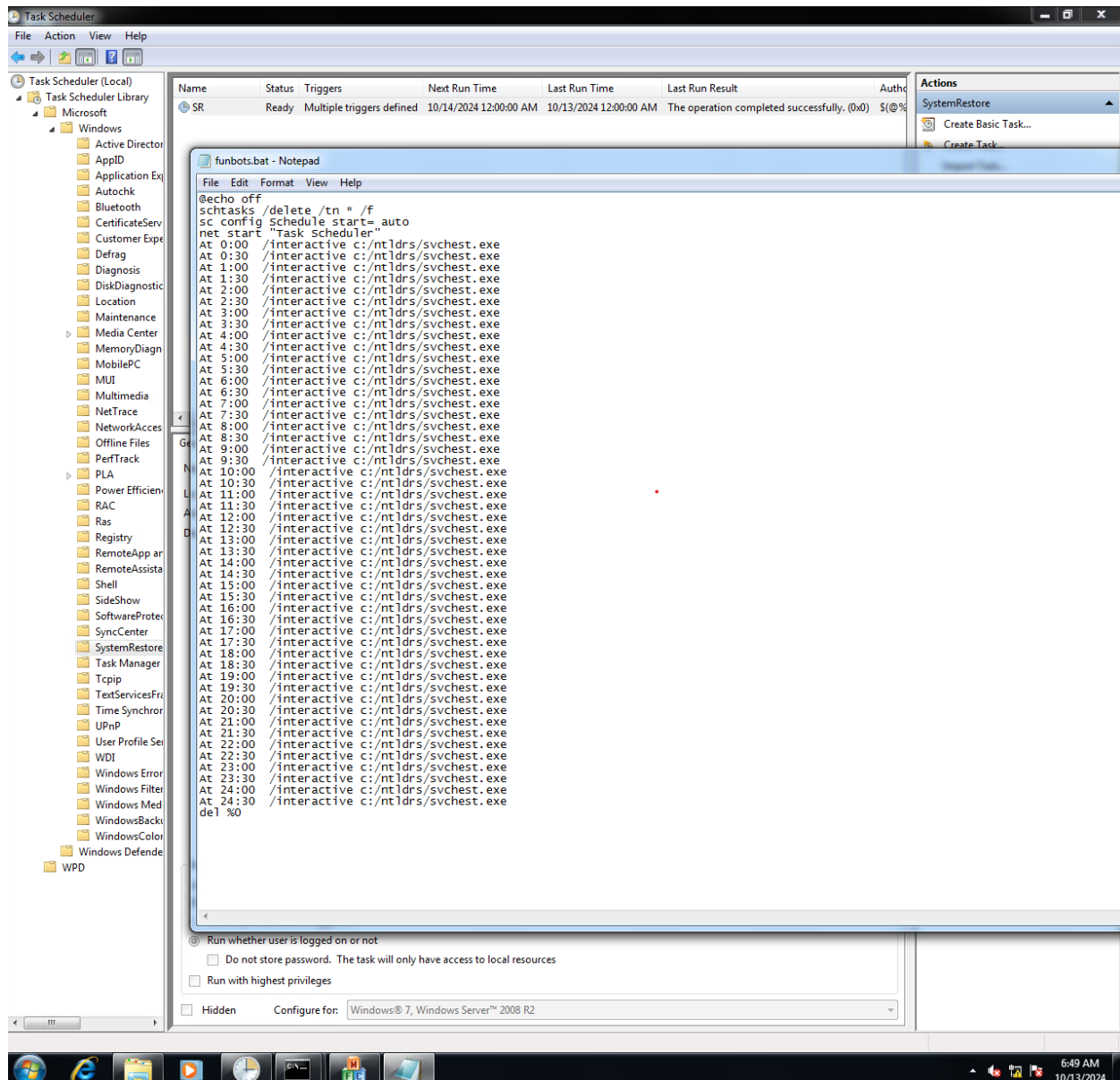


Figure 7

Dive Deeper into the funbots.bat using Notepad, there is a Task Scheduler that will run the file svchost.exe every 30 mins.

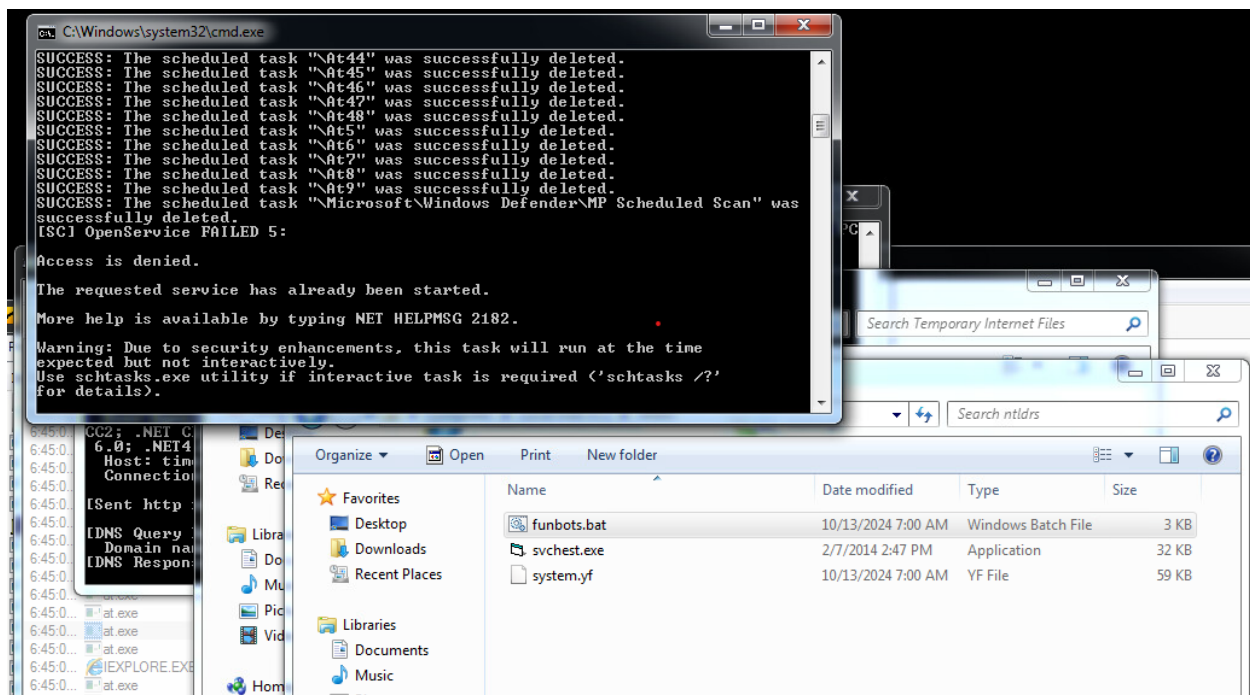


Figure 8

Execute tongji2.exe will pop-up the same notification as evil.exe but will also pop-up a cmd that does not show any information.

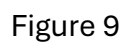


Figure 9

By using Process Explorer, I see there is a clone of Internet Explorer running, which is iexplore.exe

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe	0.01	10,012 K	10,656 K	1268	Host Process for Windows S...	Microsoft Corporation
VGAAuthService.exe		4,916 K	8,960 K	1484	VMware Guest Authenticatio...	VMware, Inc.
vmtoolsd.exe	0.03	7,144 K	15,076 K	1608	VMware Tools Core Service	VMware, Inc.
taskhost.exe		2,856 K	6,412 K	1692	Host Process for Windows T...	Microsoft Corporation
dllhost.exe	< 0.01	2,980 K	8,588 K	1088	COM Surrogate	Microsoft Corporation
msdtc.exe		2,544 K	6,308 K	1760	Microsoft Distributed Transa...	Microsoft Corporation
SearchIndexer.exe		17,736 K	11,616 K	2184	Microsoft Windows Search I...	Microsoft Corporation
WmiApSrv.exe		2,000 K	5,040 K	2564	WMI Performance Reverse ...	Microsoft Corporation
svchost.exe		712 K	1,964 K	3304	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	1,644 K	4,916 K	112	Host Process for Windows S...	Microsoft Corporation
sppsvc.exe		1,968 K	4,096 K	2436	Microsoft Software Protectio...	Microsoft Corporation
svchost.exe		102,548 K	6,544 K	2456	Host Process for Windows S...	Microsoft Corporation
wmpnetwk.exe	< 0.01	3,220 K	1,600 K	2644	Windows Media Player Netw...	Microsoft Corporation
lsass.exe	< 0.01	3,080 K	7,384 K	532	Local Security Authority Proc...	Microsoft Corporation
lsn.exe	< 0.01	1,124 K	2,852 K	540	Local Session Manager Serv...	Microsoft Corporation
csrss.exe	0.04	7,484 K	10,944 K	428	Client Server Runtime Process	Microsoft Corporation
conhost.exe		1,156 K	5,056 K	3144	Console Window Host	Microsoft Corporation
winlogon.exe		1,668 K	4,716 K	472	Windows Logon Application	Microsoft Corporation
explorer.exe		56,532 K	60,928 K	1624	Windows Explorer	Microsoft Corporation
vmtoolsd.exe	0.06	3,780 K	8,544 K	2024	VMware Tools Core Service	VMware, Inc.
flypaper.exe		1,016 K	4,896 K	2832	TODO: <File description>	TODO: <Company name>
proccxp.exe	0.39	66,536 K	75,168 K	2904	Sysinternals Process Explorer	Sysinternals - www.sysinter...
Procmon.exe	0.23	22,992 K	28,564 K	2940	Process Monitor	Sysinternals - www.sysinter...
AntiSpy.exe		7,808 K	16,284 K	3032	Anti Virus & Rootkit Tools	AntiSpy@163.com
FakeNet.exe		5,532 K	8,568 K	3136		
ipconfig.exe		216 K	220 K	3212	IP Configuration Utility	Microsoft Corporation
iexplore.exe		7,720 K	19,876 K	3708	Internet Explorer	Microsoft Corporation
iexplore.exe	< 0.01	4,448 K	15,688 K	3836	Internet Explorer	Microsoft Corporation

CPU Usage: 1.99% Commit Charge: 18.95% Processes: 44 Physical Usage: 26.38%

Figure 10

Conclusion

After looking at the file evil.exe using all the tool above, I can say the file evil.exe do the following:

- Adding dangerous files, such as funbots.bat to execute on a particular time.
- Point user to a specific host, which runs whenever user turns on their computer.
- The program then downloads multiple files from timeless888.com and hishunpharm.com
- The program then becomes an Internet Explorer clone, which runs whenever the original Internet Explorer runs.
- The cycle will keep continue and user will have a difficult time in delete them since there is a scheduled action to re-run them