Practical Assignment 1 Report

02/19/2020

Justin Miller: miller.j@ufl.edu

Assignment P0x01

CIS4930-108A(2506)

Table of Contents

Executive Summary

The malware sample that was provided seems to be some form of trojan belonging to the Carberp family of trojans. The malware repeatedly sends requests over the network to three different Command and Control(C&C) servers. The malware does not appear to perform any malicious activity without first successfully connecting to one of the C&C servers.

After running the malware, it will copy itself to a windows startup directory to achieve persistence and delete the original executable. It will then spawn a process that imitates svchost.exe which creates some temp files and a directory in C:\ containing a .dat and .inf file. Indicators of compromise are the existence of the copied executable in a windows startup directory, some specific files and directories being created, and the network requests to the C&C server.

Static Analysis

Basic Static Analysis

Initial analysis of the program was done using PEStudio, which provides a detailed breakdown of portable executable (PE) files. The compiler stamp shows the malware was compiled on November 19th, 2008, though this may have been modified by the malware creator.

compiler-stamp	0x4924BC43 (Wed Nov 19 20:24:19 2008)

PEStudio was also able to identify that this program as a Windows GUI program rather than a Command-line program.

subsystem	GUI

Regarding packing, PEStudio does not recognize a signature for a packer and there is a high number of imports and strings that are being found though which typically indicates that the malware is less likely to be packed. However, the entropy of the text section is substantially over 7. High entropy values, between 7 and 8, indicate that an executable is most likely packed. Based on just this information it is likely that the program is packed.

property	value	value	value	value	value
name	.text	.rdata	.data	.rsrc	.reloc
md5	F09D2536AE870ED5B64B955...	020E34F80C467FFB1BC01CD...	6B13C848F593A48F5059FAA...	4B56ECCC0E70AE95918987F...	B29DF4118B6429018C6F062...
entropy	7.727	7.920	7.862	2.727	5.268
file-ratio (99.35%)	49.51 %	35.50 %	12.70 %	0.65 %	0.98 %
raw-address	0x00000400	0x00013400	0x00020E00	0x00025C00	0x00026000
raw-size (156160 bytes)	0x00013000 (77824 bytes)	0x0000DA00 (55808 bytes)	0x00004E00 (19968 bytes)	0x00000400 (1024 bytes)	0x00000600 (1536 bytes)
virtual-address	0x00401000	0x00414000	0x00422000	0x0044E000	0x0044F000
virtual-size (313856 bytes)	0x00013000 (77824 bytes)	0x0000DA00 (55808 bytes)	0x0002B600 (177664 bytes)	0x00000400 (1024 bytes)	0x00000600 (1536 bytes)
entry-point	0x00011710	-	-	-	-
characteristics	0x60000020	0x40000040	0xC0000040	0x40000040	0x42000040
writable	-	-	x	-	-
executable	x	-	-	-	-
shareable	-	-	-	-	-
discardable	-	-	-	-	x
initialized-data	-	x	x	x	x
uninitialized-data	-	-	-	-	-
unreadable	-	-	-	-	-
self-modifying	-	-	-	-	-
virtualized	-	-	-	-	-
file	n/a	n/a	n/a	n/a	n/a

The imports section of PEStudio finds many functions which are imported from various libraries. Some interesting functions are LoadLibraryA, and various functions from wininet.dll, ws2_32.dll, and wldap32.dll. From these libraries being included it seems likely that the program will probably try to perform network activity. It is strange that there are so many libraries found in malware that is likely packed.

name (224)	group (14)	type (1)	ordinal (0)	blacklist (132)
LoadLibraryA	dynamic-library	implicit	-	-
LoadUrlCacheContent	network	implicit	-	x
LocalCompact	memory	implicit	-	x
LockFileEx	file	implicit	-	x

name (224)	group (14)	type (1)	ordinal (0)	blacklist (132)	anti-debug (0)	undocumented (5)	deprecated (10)	library (6)
FindFirstUrlCacheContai...	network	implicit	-	x	-	x	-	wininet.dll
InternetSetCookieExW	network	implicit	-	x	-	-	-	wininet.dll
InternetCloseHandle	network	implicit	-	x	-	-	-	wininet.dll
InternetSecurityProtocol...	network	implicit	-	x	-	x	-	wininet.dll
InternetTimeFromSyste...	network	implicit	-	x	-	-	-	wininet.dll

name (224)	group (14)	type (1)	ordinal (0)	blacklist (132)	anti-debug (0)	undocumented (5)	deprecated (10)	library (6)
WSALookupServiceEnd	network	implicit	-	x	-	-	-	ws2_32.dll
WSARecvFrom	network	implicit	-	x	-	-	-	ws2_32.dll
WSAInstallServiceClassA	network	implicit	-	x	-	-	-	ws2_32.dll
WSAAsyncGetServByPort	network	implicit	-	x	-	-	-	ws2_32.dll
WSACancelBlockingCall	network	implicit	-	x	-	-	-	ws2_32.dll
WSALookupServiceBeginA	network	implicit	-	x	-	-	-	ws2_32.dll
ntohl	network	implicit	-	x	-	-	-	ws2_32.dll

name (224)	group (14)	type (1)	ordinal (0)	blacklist (132)	anti-debug (0)	undocumented (5)	deprecated (10)	library (6)
ldap_count_values	directory	implicit	-	x	-	-	-	wldap32.dll
ldap_create_sort_controlW	directory	implicit	-	x	-	-	-	wldap32.dll
ldap_create_vlv_controlA	directory	implicit	-	x	-	-	-	wldap32.dll
ldap_delete	directory	implicit	-	x	-	-	-	wldap32.dll
ldap_delete_sW	directory	implicit	-	x	-	-	-	wldap32.dll
ldap_explode_dnW	directory	implicit	-	x	-	-	-	wldap32.dll

Looking through the strings section of PEStudio does not provide any relevant information, the only readable string that are found are function names and the names of the imported dlls.

type (2)	size (bytes)	file-offset	blacklist (96)	hint (10)	group (16)	value (1759)
ascii	6	0x00013916	x	-	compression	LZInit
ascii	25	0x00013726	x	-	-	CancelDeviceWakeupRequest
ascii	22	0x00013A18	x	-	-	SetTimeZoneInformation
ascii	4	0x00006631	-	utility	-	exec
ascii	10	0x00013B90	-	file	network	WS2_32.dll
ascii	11	0x000142B6	-	file	network	WININET.dll
ascii	11	0x00013E26	-	file	directory	WLDAP32.dll

The program sections also do not provide much information useful to analysis aside from the entropy indicating it likely being packed.

Virus Total

After performing analysis in PEStudio, the malware sample was hashed and uploaded to VirusTotal, a site which checks the hash against many malware detection engines. A very high number of these engines detected the program as malware. Of the engines that recognized the program as malware there were many that recognized it as a Trojan, and a few recognized as belonging to the Carberp family of trojans.

58 / 70

Community Score

58 engines detected this file

a67a1ca66f666eabef466bd6beba25867fd67ba697c1c7c02cde2c51e4e8289d

KayU1y

direct-cpu-clock-access | long-sleeps | nxdomain | peexe | runtime-modules

153.50 KB
Size

2021-02-05 00:16:05 UTC
10 days ago

EXE

Acronis	Suspicious	Ad-Aware	Gen:Heur.Zygug.1
AegisLab	Trojan.Win32.Generic.4!c	AhnLab-V3	Win-Trojan/Malpacked3.Gen
Alibaba	Trojan:Win32/Ramdo.aa9a5f1c	Antiy-AVL	Trojan[Spy]/Win32.Carberp
SecureAge APEX	Malicious	Arcabit	Trojan.Zygug.1
Avast	Win32:FakeAlert-CJO [Trj]	AVG	Win32:FakeAlert-CJO [Trj]
Avira (no cloud)	TR/Crypt.ZPACK.Gen	BitDefender	Gen:Heur.Zygug.1
BitDefenderTheta	Gen:NN.ZexaF.34804.ju0@aSX6fdoi	CAT-QuickHeal	Trojan.Generic
Comodo	Malware@#1fniabscm86bj	CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cybereason	Malicious.32fd84	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Ransom.UVFD-2660

Virus Total also provides a list of hashes and other properties of the program, which identifies the program as a Windows 32-bit executable file.

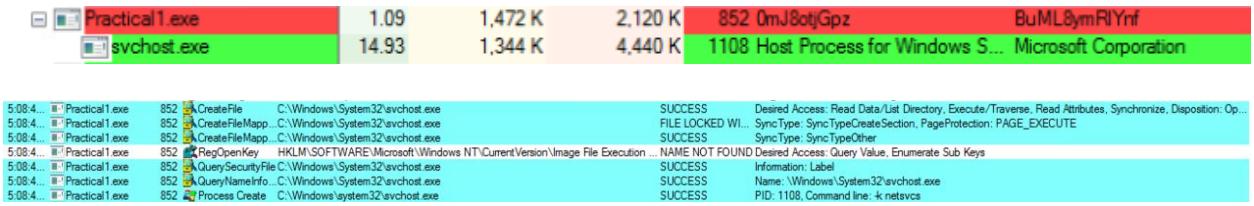
Basic Properties

MD5	3ea4b7a32fd84202938e79616a223832
SHA-1	59a72240bba9233a1d37b96d86b432d678380e38
SHA-256	a67a1ca66f666eabef466bd6beba25867fd67ba697c1c7c02cde2c51e4e8289d
Vhash	015056757d75155az57qz2300227z
Authentihash	f1ddc42298039028e3e7273c0156c6f6945af6de8bc3cb20cc7d7f05c2972b9a
Imphash	e914ee5933dcbf97ecfbcd451d87890d
SSDEEP	3072:0d6bnzbZZvufCrkR/K25KeqDYNdf4Z5x8M5+Kb4V9pDVor:0d6vbZZG6rktKyTkCfQx8M5+E4VDs
TLSH	T133E302B3FD503627F80A64B91677E326A33937B103B38319BA955A8535E6EC5A805313
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win64 Executable (generic) (28.6%)
TrID	Win16 NE executable (generic) (19.1%)
TrID	Win32 Dynamic Link Library (generic) (17.8%)
TrID	Win32 Executable (generic) (12.2%)
TrID	Win16/32 Executable Delphi generic (5.6%)
File size	153.50 KB (157184 bytes)

Dynamic Analysis

Process Behaviors

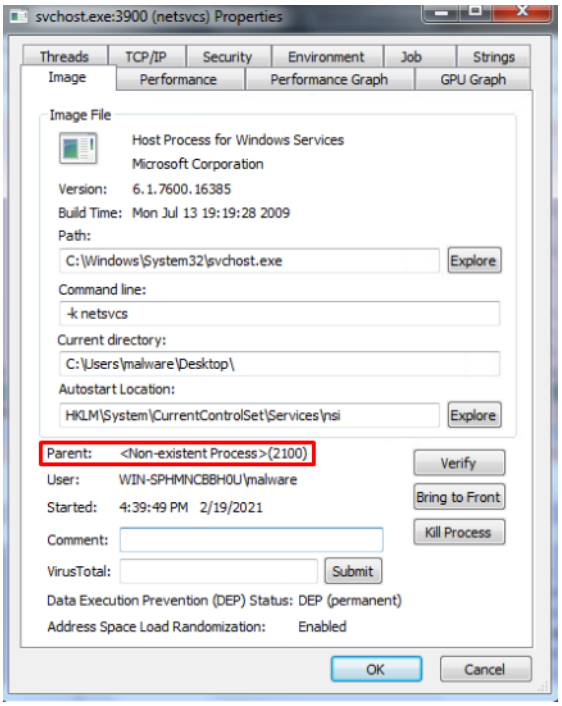
When the malware is run the executable Practical1.exe is visible in process explorer for a short amount of time. In that time, it spawns an instance of svchost.exe and after a few seconds the Practical1.exe process is stopped while the svchost.exe process continues to execute.



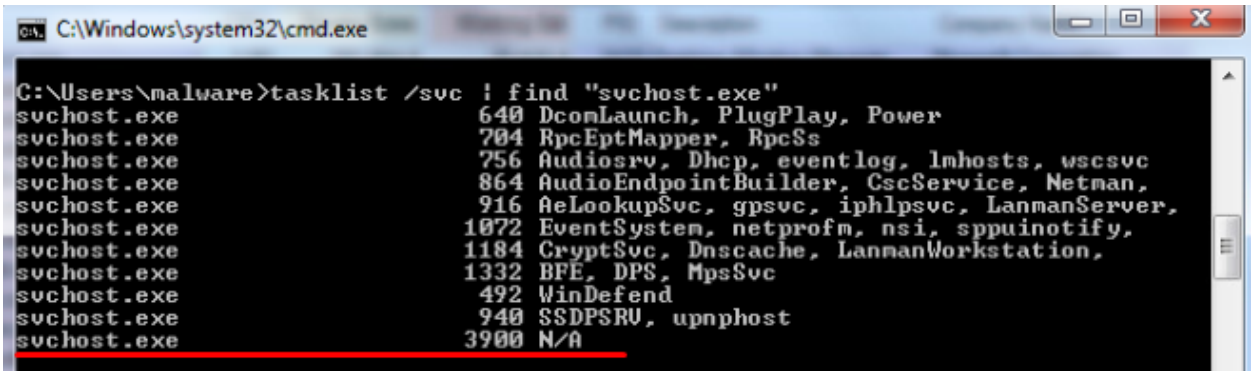
Practical1.exe	1.09	1,472 K	2,120 K	852	0mJ8otjGpz	BuML8ymRlYnf
svchost.exe	14.93	1,344 K	4,440 K	1108	Host Process for Windows S...	Microsoft Corporation

5:08:4...	Practical1.exe	852	CreateFile	C:\Windows\System32\svchost.exe	SUCCESS	Desired Access: Read Data/List Directory, Execute/Traverse, Read Attributes, Synchronize, Disposition: Op...
5:08:4...	Practical1.exe	852	CreateFileMapp...	C:\Windows\System32\svchost.exe	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE
5:08:4...	Practical1.exe	852	CreateFileMapp...	C:\Windows\System32\svchost.exe	SUCCESS	SyncType: SyncTypeOther
5:08:4...	Practical1.exe	852	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution ...	NAME NOT FOUND	Desired Access: Query Value, Enumerate Sub Keys
5:08:4...	Practical1.exe	852	QuerySecurityFile	C:\Windows\System32\svchost.exe	SUCCESS	Information: Label
5:08:4...	Practical1.exe	852	QueryNameInfo...	C:\Windows\System32\svchost.exe	SUCCESS	Name: \Windows\System32\svchost.exe
5:08:4...	Practical1.exe	852	Process Create	C:\Windows\system32\svchost.exe	SUCCESS	PID: 1108, Command line: -k netsvcs

Once this happens the executable that was used to start the malware will be missing. Killing the svchost.exe process will stop it for a few seconds, but the process is started again after. The svchost.exe process has Non-existent Process listed as its parent and is not shown under any other processes in process explorer unlike the other instances of svchost.exe.



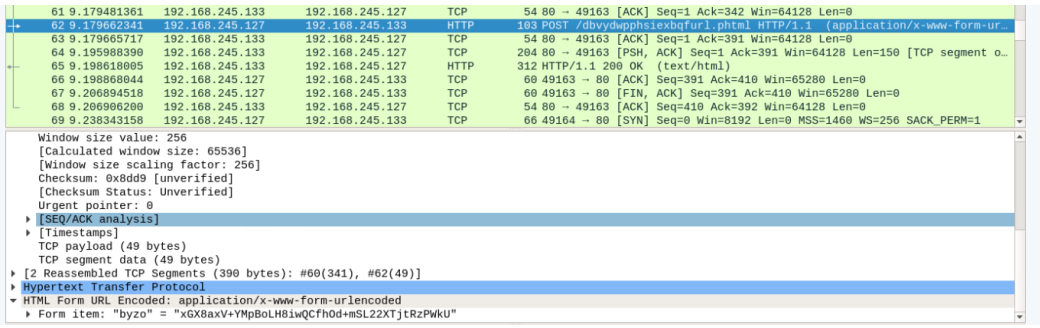
The task list shows a list of currently running processes, using the option /svc shows all the services for each process. Using a pipe to filter for svchost.exe shows the services being hosted by each instance of svchost.exe, the instance that was started by the malware has an N/A for the tasks meaning it is not actually hosting any services as it would be expected of an instance of svchost.exe to be doing.



Network Activity

Using FakeDNS to spoof DNS responses showed the domains that the malware was attempting to reach. There are three separate domains that are looped through until it can make a connection to one of them. These are likely the C&C servers which the malware contacts to send information to or receive instructions from.

Running INetSim and using Wireshark to capture packets showed some interesting requests being made. When a successful connection to one of the C&C servers was simulated with INetSim, the malware stopped sending TCP requests trying to find the other C&C server and began sending HTTP requests to the one it connected to. The requests are made to a .phtml page and have a form item attached that looks like base64 but trying to decode it using Burp Suite's Decoder tool was not successful.

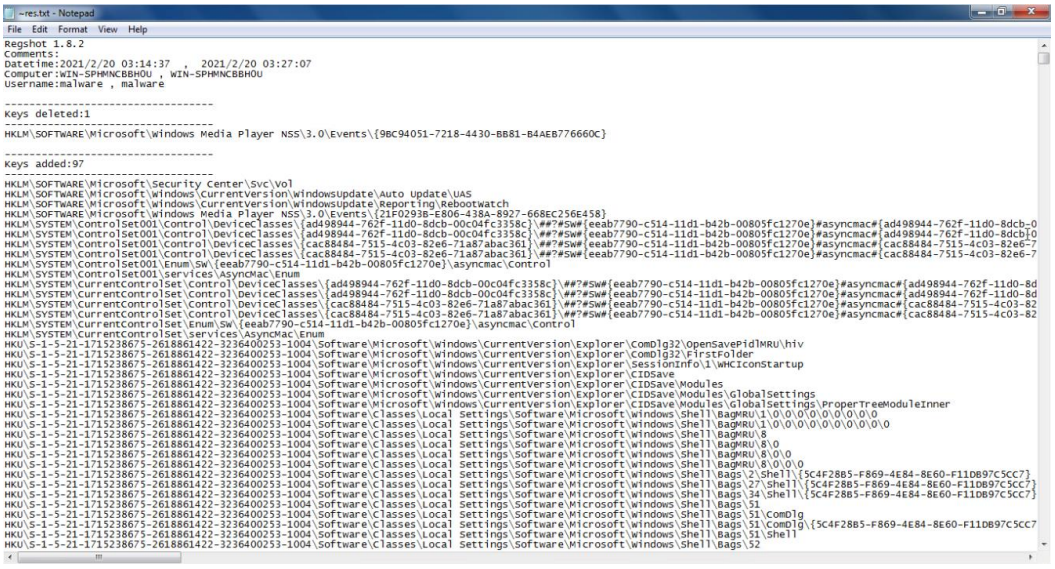


61	9.179481361	192.168.245.133	192.168.245.127	TCP	54	80 → 49163 [ACK] Seq=1 Ack=342 Win=64128 Len=0
62	9.179662341	192.168.245.127	192.168.245.133	HTTP	103	POST /dbvydwpphsiexbqfurl.phtml HTTP/1.1 (application/x-www-ur…
63	9.179665717	192.168.245.133	192.168.245.127	TCP	54	80 → 49163 [ACK] Seq=1 Ack=391 Win=64128 Len=0
64	9.195988390	192.168.245.133	192.168.245.127	TCP	204	80 → 49163 [PSH, ACK] Seq=1 Ack=391 Win=64128 Len=150 [TCP segment o…
65	9.198618005	192.168.245.133	192.168.245.127	HTTP	312	HTTP/1.1 200 OK (text/html)
66	9.198868044	192.168.245.127	192.168.245.133	TCP	60	49163 → 80 [ACK] Seq=391 Ack=410 Win=65280 Len=0
67	9.206894518	192.168.245.127	192.168.245.133	TCP	60	49163 → 80 [FIN, ACK] Seq=391 Ack=410 Win=65280 Len=0
68	9.206906200	192.168.245.133	192.168.245.127	TCP	54	80 → 49163 [ACK] Seq=410 Ack=392 Win=64128 Len=0
69	9.238343158	192.168.245.127	192.168.245.133	TCP	66	49164 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

```
Window size value: 256
[Calculated window size: 65536]
[Window size scaling factor: 256]
Checksum: 0x8dd9 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
▸ [SEQ/ACK analysis]
▸ [Timestamps]
TCP payload (49 bytes)
TCP segment data (49 bytes)
▸ [2 Reassembled TCP Segments (390 bytes): #60(341), #62(49)]
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "byzo" = "xGX8axV+YMpBoLH8iwQCfhOd+mSL22XTjtRzPWkU"
```

Registry Keys

There does not seem to be too much interesting registry activity. Using RegShot before and after running the malware and comparing the two shot showed a lot of registry changes but not any that seemed very compromising on inspection.



```
~res.txt - Notepad
File  Edit  Format  View  Help
Regshot 1.8.2
Comments:
Datetime:2021/2/20 03:14:37 , 2021/2/20 03:27:07
Computer:WIN-SPHMNCBBHOU , WIN-SPHMNCBBHOU
Username:malware , malware

----------------------------------
Keys deleted:1
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows Media Player NSS\3.0\Events\{9BC94051-7218-4430-BB81-B4AEB776660C}

----------------------------------
Keys added:97
----------------------------------
HKLM\SOFTWARE\Microsoft\Security Center\Svc\Vol
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\UAS
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Reporting\RebootWatch
HKLM\SOFTWARE\Microsoft\Windows Media Player NSS\3.0\Events\{21F0293B-E806-438A-8927-668EC256E458}
HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#SW#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-8dcb-0
HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#SW#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-8dcb10
HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#SW#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-82e6-7
HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#SW#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-82e6-7
HKLM\SYSTEM\ControlSet001\Enum\SW\{eeab7790-c514-11d1-b42b-00805fc1270e}\asyncmac\Control
HKLM\SYSTEM\ControlSet001\services\AsyncMac\Enum
HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#SW#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-8d
HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#SW#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-8d
HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#SW#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-82
HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#SW#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-82
HKLM\SYSTEM\CurrentControlSet\Enum\SW\{eeab7790-c514-11d1-b42b-00805fc1270e}\asyncmac\Control
HKLM\SYSTEM\CurrentControlSet\services\AsyncMac\Enum
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\hiv
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\FirstFolder
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\WHCIconStartup
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\CIDSave
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\CIDSave\Modules
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\CIDSave\Modules\GlobalSettings
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\CIDSave\Modules\GlobalSettings\ProperTreeModuleInner
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\0\0\0\0\0\0\0
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\0\0\0\0\0\0\0\0\0
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\8
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\8\0
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\8\0\0
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\8\0\0\0
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\2\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\27\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\34\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\51
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\51\ComDlg
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\51\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\51\Shell
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\52
```

Filesystem Activity

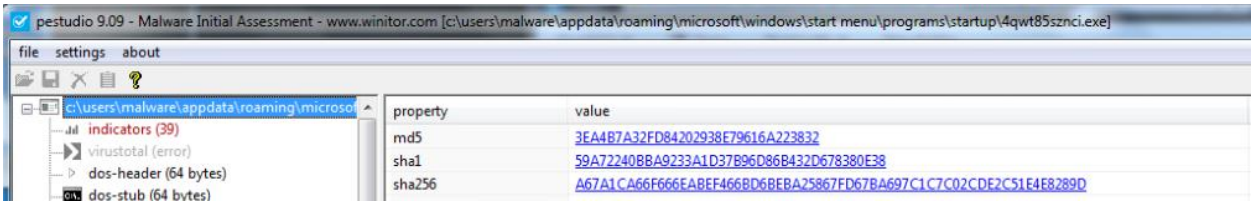
The most obvious filesystem activity is that the executable of the malware is deleted. Using ProcMon to monitor changes to files also provided a log of this deletion happening.

5:08:4...	Explorer.EXE	2216	CreateFile	C:\Users\malware\Desktop\Practical1.exe	SUCCESS	Desired Access: Write Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Open ...
5:08:4...	Explorer.EXE	2216	SetBasicInform...	C:\Users\malware\Desktop\Practical1.exe	SUCCESS	CreationTime: 0, LastAccessTime: 0, LastWriteTime: 0, ChangeTime: 0, FileAttributes: AN
5:08:4...	Explorer.EXE	2216	NotifyChangeDi...	C:\Users\malware\Desktop	SUCCESS	Filter: FILE_NOTIFY_CHANGE_FILE_NAME, FILE_NOTIFY_CHANGE_ATTRIBUTES, FILE_NOTIFY_CHA...
5:08:4...	Explorer.EXE	2216	CloseFile	C:\Users\malware\Desktop\Practical1.exe	SUCCESS	
5:08:4...	Explorer.EXE	2216	CreateFile	C:\Users\malware\Desktop\Practical1.exe	SUCCESS	Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Poin...
5:08:4...	Explorer.EXE	2216	QueryAttributeT...	C:\Users\malware\Desktop\Practical1.exe	SUCCESS	Attributes: A, ReparseTag: 0x0
5:08:4...	Explorer.EXE	2216	SetDispositionI...	C:\Users\malware\Desktop\Practical1.exe	SUCCESS	Delete: True
5:08:4...	Explorer.EXE	2216	CloseFile	C:\Users\malware\Desktop\Practical1.exe	SUCCESS	

ProcMon showed a lot of activity in the C:\Users\{user}\AppData\Microsoft\Start Menu\Programs\Startup folder, including the creation of a .exe file. This startup folder will run whatever programs are in it when Windows startups.

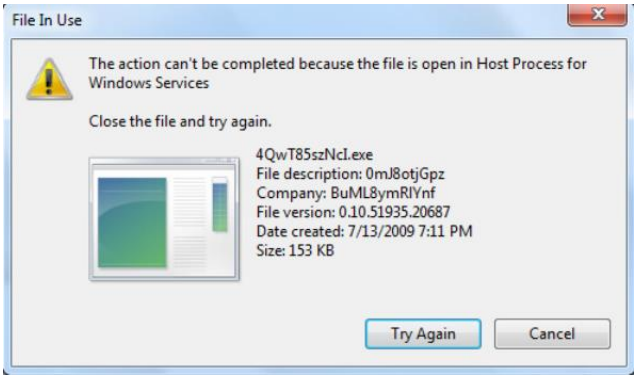
6:24:2...	Explorer.EXE	1260	CreateFile	C:\Users\malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini	SUCCESS	Desired Access: G...
6:24:2...	Explorer.EXE	1260	QueryStandardI...	C:\Users\malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini	SUCCESS	AllocationSize: 176...
6:24:2...	Explorer.EXE	1260	ReadFile	C:\Users\malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini	SUCCESS	Offset: 0, Length: 1...
6:24:2...	Explorer.EXE	1260	QueryBasicInfor...	C:\Users\malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini	SUCCESS	CreationTime: 1/14...
6:24:2...	Explorer.EXE	1260	CloseFile	C:\Users\malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini	SUCCESS	
6:24:2...	Explorer.EXE	1260	CreateFile	C:\Users\malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	SUCCESS	Desired Access: R...
6:24:2...	Explorer.EXE	1260	FileSystemControl	C:\Users\malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	INVALID DEVICE ...	Control: FSCTL_L...
6:24:2...	Explorer.EXE	1260	QueryDirectory	C:\Users\malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	SUCCESS	0: ., 1: .., 2: 4QwT...
6:24:2...	Explorer.EXE	1260	QueryDirectory	C:\Users\malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	NO MORE FILES	
6:24:2...	Explorer.EXE	1260	CloseFile	C:\Users\malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	SUCCESS	
6:24:2...	Explorer.EXE	1260	CreateFile	C:\Users\malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\4QwT85szNcI.exe	SUCCESS	Desired Access: G...
6:24:2...	Explorer.EXE	1260	QuerySecurityFile	C:\Users\malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\4QwT85szNcI.exe	SUCCESS	Information: Owner...
6:24:2...	Explorer.EXE	1260	QueryBasicInfor...	C:\Users\malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\4QwT85szNcI.exe	SUCCESS	CreationTime: 7/13...
6:24:2...	Explorer.EXE	1260	CreateFile	C:\Users\malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\4QwT85szNcI.exe	SUCCESS	Desired Access: G...
6:24:2...	Explorer.EXE	1260	CreateFileMapp...	C:\Users\malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\4QwT85szNcI.exe	FILE LOCKED WI...	SyncType: SyncTy...
6:24:2...	Explorer.EXE	1260	CreateFileMapp...	C:\Users\malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\4QwT85szNcI.exe	SUCCESS	SyncType: SyncTy...
6:24:2...	Explorer.EXE	1260	CreateFile	C:\Users\malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\4QwT85szNcI.exe....	NAME NOT FOUND	Desired Access: G...
6:24:2...	Explorer.EXE	1260	CloseFile	C:\Users\malware\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\4QwT85szNcI.exe	SUCCESS	

Looking at the executable that was dropped in PEStudio shows that the hash is the same as the original executable. This means that this executable is the malware copying itself to the startup directory to achieve persistence, it may be necessary to uncheck “Hide protected operating system files” in Folder Options for this executable to be visible.

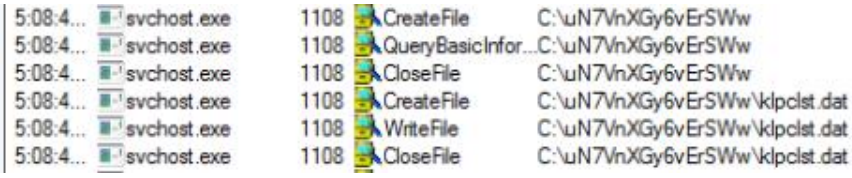


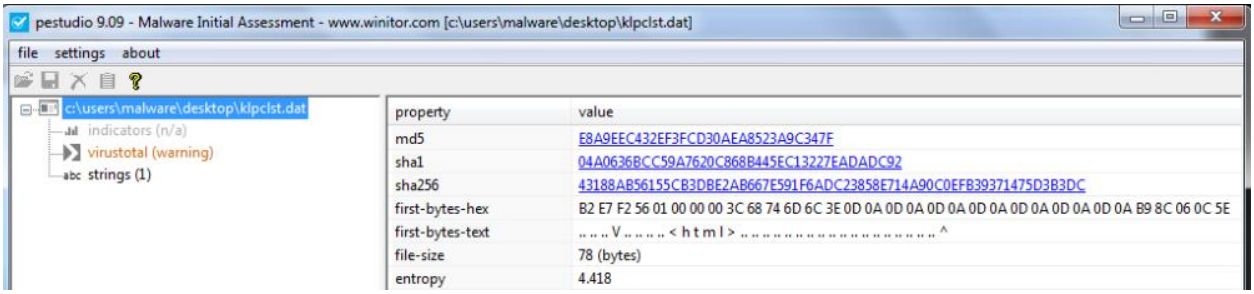
Deleting this dropped executable will stop the malware from running again when the computer is restarted. If the computer is restarted after the malware has been run this executable attempting

to delete the executable will give a notice the file is open but killing the malicious svchost.exe process gives a short window of time to delete the executable which will stop the malware once the computer has restarted.

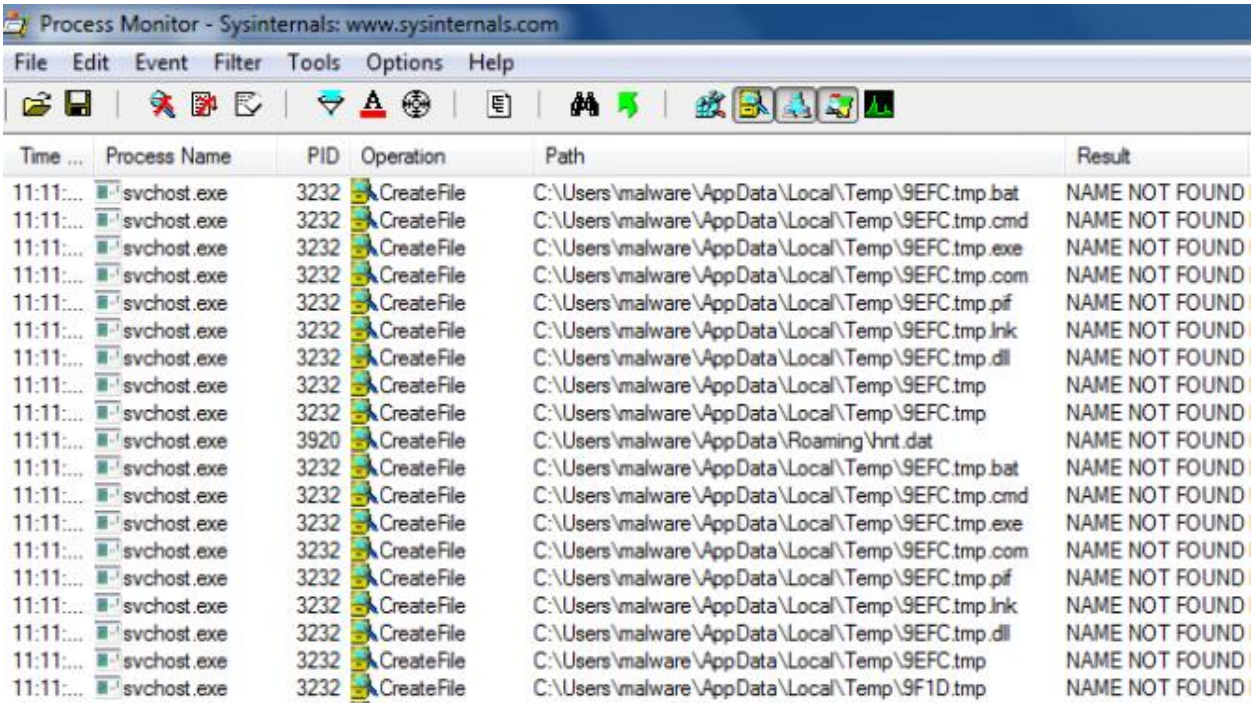


There are a few files that get created within a folder in C:\ which seem to be created and deleted often by the malware. Neither of the files contain anything that can be easily interpreted, though klpcst.dat seems to be a static file, has the same hash on multiple runs.





There are a lot of files that the malware attempts to open but fails because they do not exist, mostly various temp files in AppData\Local\Temp as well as a “hnt.dat” in AppData\Roaming.



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result
11:11:...	svchost.exe	3232	CreateFile	C:\Users\malware\AppData\Local\Temp\9EFC.tmp.bat	NAME NOT FOUND
11:11:...	svchost.exe	3232	CreateFile	C:\Users\malware\AppData\Local\Temp\9EFC.tmp.cmd	NAME NOT FOUND
11:11:...	svchost.exe	3232	CreateFile	C:\Users\malware\AppData\Local\Temp\9EFC.tmp.exe	NAME NOT FOUND
11:11:...	svchost.exe	3232	CreateFile	C:\Users\malware\AppData\Local\Temp\9EFC.tmp.com	NAME NOT FOUND
11:11:...	svchost.exe	3232	CreateFile	C:\Users\malware\AppData\Local\Temp\9EFC.tmp.pif	NAME NOT FOUND
11:11:...	svchost.exe	3232	CreateFile	C:\Users\malware\AppData\Local\Temp\9EFC.tmp.lnk	NAME NOT FOUND
11:11:...	svchost.exe	3232	CreateFile	C:\Users\malware\AppData\Local\Temp\9EFC.tmp.dll	NAME NOT FOUND
11:11:...	svchost.exe	3232	CreateFile	C:\Users\malware\AppData\Local\Temp\9EFC.tmp	NAME NOT FOUND
11:11:...	svchost.exe	3232	CreateFile	C:\Users\malware\AppData\Local\Temp\9EFC.tmp	NAME NOT FOUND
11:11:...	svchost.exe	3920	CreateFile	C:\Users\malware\AppData\Roaming\hnt.dat	NAME NOT FOUND
11:11:...	svchost.exe	3232	CreateFile	C:\Users\malware\AppData\Local\Temp\9EFC.tmp.bat	NAME NOT FOUND
11:11:...	svchost.exe	3232	CreateFile	C:\Users\malware\AppData\Local\Temp\9EFC.tmp.cmd	NAME NOT FOUND
11:11:...	svchost.exe	3232	CreateFile	C:\Users\malware\AppData\Local\Temp\9EFC.tmp.exe	NAME NOT FOUND
11:11:...	svchost.exe	3232	CreateFile	C:\Users\malware\AppData\Local\Temp\9EFC.tmp.com	NAME NOT FOUND
11:11:...	svchost.exe	3232	CreateFile	C:\Users\malware\AppData\Local\Temp\9EFC.tmp.pif	NAME NOT FOUND
11:11:...	svchost.exe	3232	CreateFile	C:\Users\malware\AppData\Local\Temp\9EFC.tmp.lnk	NAME NOT FOUND
11:11:...	svchost.exe	3232	CreateFile	C:\Users\malware\AppData\Local\Temp\9EFC.tmp.dll	NAME NOT FOUND
11:11:...	svchost.exe	3232	CreateFile	C:\Users\malware\AppData\Local\Temp\9EFC.tmp	NAME NOT FOUND
11:11:...	svchost.exe	3232	CreateFile	C:\Users\malware\AppData\Local\Temp\9F1D.tmp	NAME NOT FOUND

Indicators of Compromise

Host based:

Copy of the malware stored in C:\Users\{user}\AppData\Microsoft\Start Menu\Programs\Startup

MD5 3ea4b7a32fd84202938e79616a223832

SHA-1 59a72240bba9233a1d37b96d86b432d678380e38

SHA-256 a67a1ca66f666eabef466bd6beba25867fd67ba697c1c7c02cde2c51e4e8289d

Existence of C:\uN7VnXGy6vErSWw\klpclst.dat (unreliable, only exists for a short time)

MD5 E8A9EEC432EF3FCD30AEA8523A9C347F

SHA1 04A0636BCC59A7620C88B446EC13227EADADC92

SHA266 43188AB56155CB3DBE2AB667E591F6ADC23858E714A90C0EFB39371475D3B3DC

Network based:

Attempted TCP connection or DNS query to:

- fromamericawhichlov.com
- hillaryklinton.com
- malborofrientro.com

HTTP posts containing a single form item with a short key and a long string of characters numbers and symbols