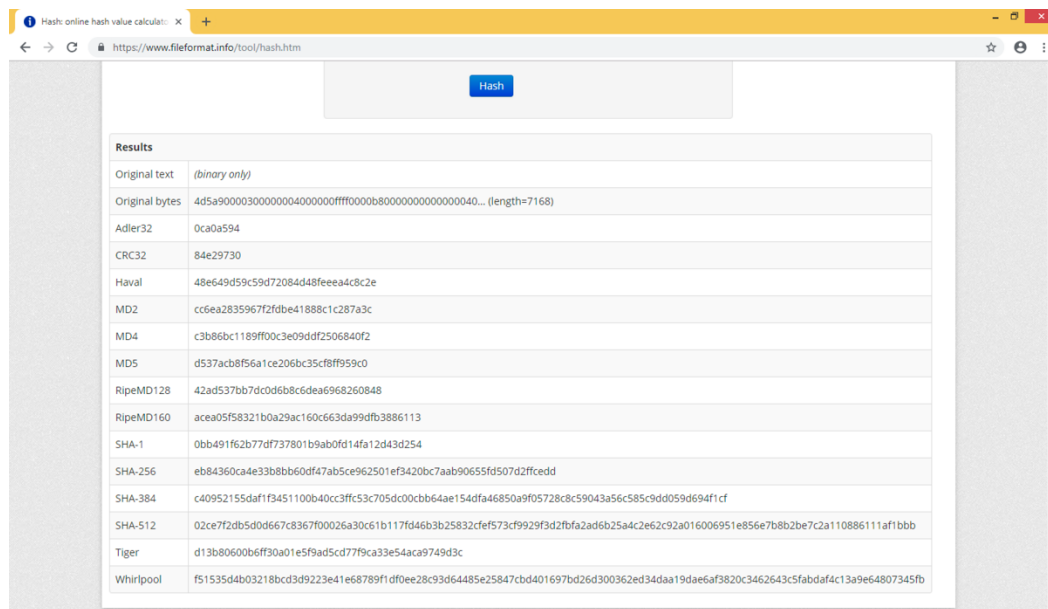


The purpose of this lab is to use all of the basic static and dynamic tools we have covered in class to construct our own examples of usage. For this lab, I am going to use the “Lab03-01” from the Chapter_3L folder provided in the malware analysis labs.

STATIC TOOLS/ANALYSIS:

The first thing I did was find the hashes using an online tool. The image below shows all the different hashes.



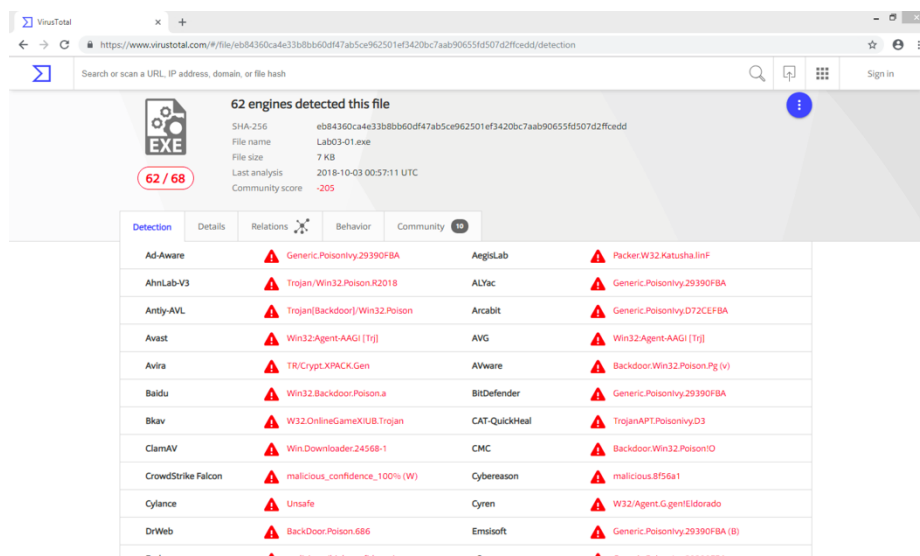
Hash online hash value calculator: X

https://www.fileformat.info/tool/hash.htm

Hash

Results	
Original text	(binary only)
Original bytes	4d5a9000030000000040000000ff0000b80000000000000040... (length=7168)
Adler32	0ca0a594
CRC32	84e29730
Haval	48e649d59c59d72084d48feea4c8c2e
MD2	cc6ea2835967f2fde41888c1c287a3c
MD4	c3b86bc1189ff00c3e09ddf2506840f2
MD5	d537acb8f56a1ce206bc35cf8ff959c0
RipeMD128	42ad537bb7dcd6b8c6dea6968260848
RipeMD160	acea05f58321b0a29ac160c663da99dfb3886113
SHA-1	0bb491f62b77df737801b9ab0fd14fa12d43d254
SHA-256	eb84360ca4e33b8bb60df47ab5ce962501ef3420bc7aab90655fd507d2ffcedd
SHA-384	c40952155daf1f3451100b40cc3ffc53c705dc00cb64ae154dfa46850a9f05728c8c59043a56c585c9dd059d694f1cf
SHA-512	02ce7f2db50d0667c8367f00026a30c61b117fd463b25832cfef573cf9929f3d2fbfa2ad6b25a4c2e62c92a016006951e856e7b8b2be7c2a110886111af1bbb
Tiger	d13b80600b6ff30a01e5f9ad5cd77f9ca33e54aca9749d3c
Whirlpool	f515354db03218bcd3d9223e41e68789f1df0ee28c93d64485e25847cbd401697bd26d300362ed34daa19dae6af3820c3462643c5fabdaf4c13a9e64807345fb

I then proceeded to analyze the file using VirusTotal to detect the type of malware. As can be seen in the image below, 62 different engines detected the file to contain malware and be of a malicious nature.



VirusTotal

https://www.virustotal.com/#/file/eb84360ca4e33b8bb60df47ab5ce962501ef3420bc7aab90655fd507d2ffcedd/detection

Search or scan a URL, IP address, domain, or file hash

62 engines detected this file

SHA-256: eb84360ca4e33b8bb60df47ab5ce962501ef3420bc7aab90655fd507d2ffcedd

File name: Lab03-01.exe


File size: 7 KB

Last analysis: 2018-10-03 00:57:11 UTC

Community score: -205

Detection	Details	Relations	Behavior	Community
Ad-Aware	Generic.Poisonivy.29390FBA		AegisLab	Packer.W32.Katusha.Inf
AhnLab-V3	Trojan/Win32.Poison.R2018		ALYac	Generic.Poisonivy.29390FBA
Antiy-AVL	Trojan(Backdoor)-Win32.Poison		Arcabit	Generic.Poisonivy.D72CEFBA
Avast	Win32:Agent-AAGI [Trj]		AVG	Win32:Agent-AAGI [Trj]
Avira	TR/Crypt.XPACK.Gen		AVware	Backdoor.Win32.Poison.Pg (v)
Baidu	Win32.Backdoor.Poison.a		BitDefender	Generic.Poisonivy.29390FBA
Bkav	W32.OnlineGameXtUB.Trojan		CAT-QuickHeal	Trojan.APT.Poisonivy.D3
ClamAV	Win.Downloader.24568-1		CMC	Backdoor.Win32.Poison.ID
CrowdStrike Falcon	malicious_confidence_100% (W)		Cybereason	malicious.BF56a1
Cylance	Unsafe		Cyren	W32/Agent.GentEldorado
DrWeb	BackDoor.Poison.686		Emsisoft	Generic.Poisonivy.29390FBA (B)
Endgame	malicious (high confidence)		eScan	Generic.Poisonivy.29390FBA

As can be seen in the details pane below, the hashes here match the hashes from the first image. Another thing to note is that the file type is a Win32 exe and is a PE32 executable.


**62 / 68**

62 engines detected this file

SHA-256	eb84360ca4e33b8bb60df47ab5ce962501ef3420bc7aab90655fd507d2ffcedd
File name	Lab03-01.exe
File size	7 KB
Last analysis	2018-10-03 00:57:11 UTC
Community score	-205

Detection

Details

Relations 

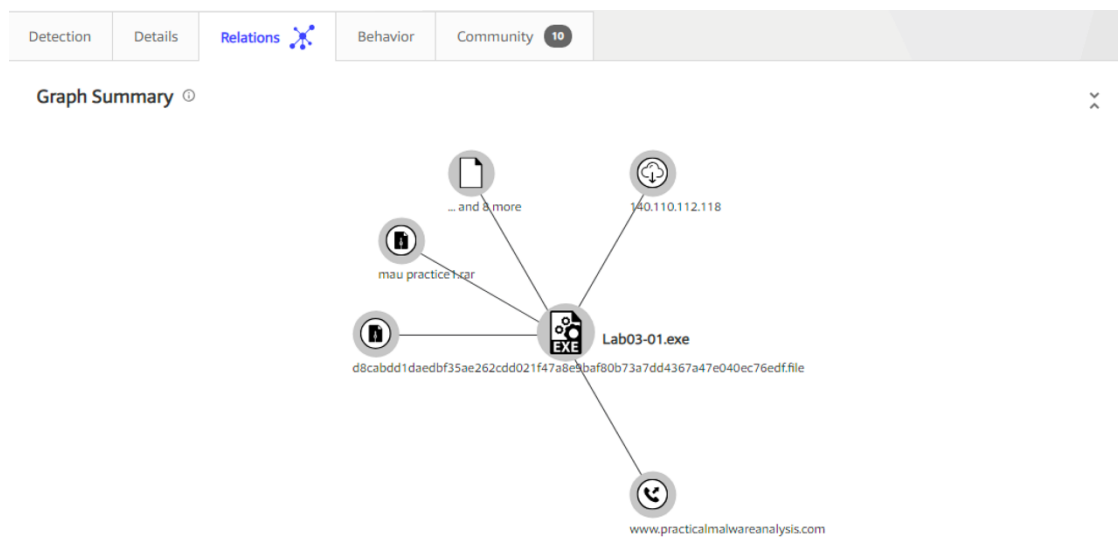
Behavior










Community **10**

Basic Properties ⓘ

MD5	d537acb8f56a1ce206bc35cf8ff959c0
SHA-1	0bb491f62b77df737801b9ab0fd14fa12d43d254
Authentihash	892e9253944a53101d7ebc249f8f9e1e616fb1f6efca00f2e689f16977172d0b
Imphash	f9ade0aa18f660a34a4fa23392e21838
File Type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
SSDeep	192:OJGc1Zl2+VAFNxl1THs6xgzgVGjPIRkTnQAx:OJGcMJxDTHfRmap
TRiD	Win32 Dynamic Link Library (generic) (38.4%) Win32 Executable (generic) (26.3%) OS/2 Executable (generic) (11.8%) Generic Win/DOS Executable (11.6%) DOS Executable Generic (11.6%)
File Size	7 KB

The image below shows the relations chart and where the malware connects to at some point during execution.

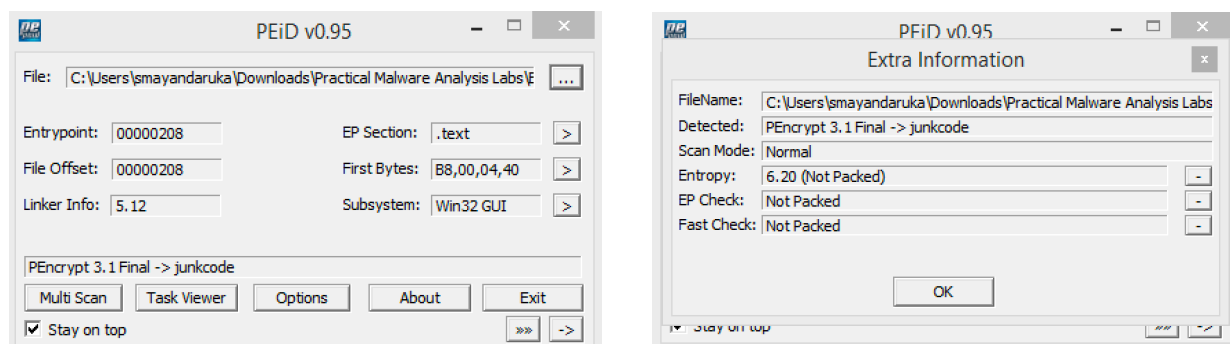


<h2>Network Communication </h2> <h3>DNS Resolutions</h3> <div>  www.practicalmalwareanalysis.com </div>	<h3>Registry Log Files </h3> <h4>Registry Keys Opened</h4> <pre> \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\996E.exe \Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option \Registry\Machine\Software\Policies\Microsoft\Windows\Safer\Codelidentifiers \REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\Codelidentifiers\TransparentEnabled \REGISTRY\USER\S-1-5-21-1482476501-1645522329-1417001333-500\Software\Policies\Microsoft\Windows\Safer\Codelidentifiers\TransparentEnabled \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ole32.dll \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\VERSION.dll \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\advpack.dll \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ntdll.dll \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KERNEL32.dll </pre> <div>  </div> <h4>Registry Keys Set</h4> <div>  \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver </div>
<h2>File System Actions </h2> <h3>Files Opened</h3> <pre> C:\WINDOWS\system32\winime32.dll C:\WINDOWS\system32\ws2_32.dll C:\WINDOWS\system32\ws2help.dll C:\WINDOWS\system32\psapi.dll C:\WINDOWS\system32\imm32.dll C:\WINDOWS\system32\lpk.dll C:\WINDOWS\system32\usp10.dll C:\WINDOWS\system32\advpack.dll C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\996E.exe C:\WINDOWS\system32\mswsock.dll C:\WINDOWS\system32\hnetcfg.dll C:\WINDOWS\system32\wshtcpip.dll </pre> <div>  </div> <h3>Files Written</h3> <pre> C:\WINDOWS\system32\vmx32to64.exe </pre>	<h2>Synchronization Mechanisms & Signals </h2> <h3>Mutexes Created</h3> <pre> WinVmx32 </pre> <h3>Modules Loaded </h3> <h4>Runtime Modules</h4> <pre> advapi32 ntdll user32 AdvpackLogFile advapi32.dll </pre>

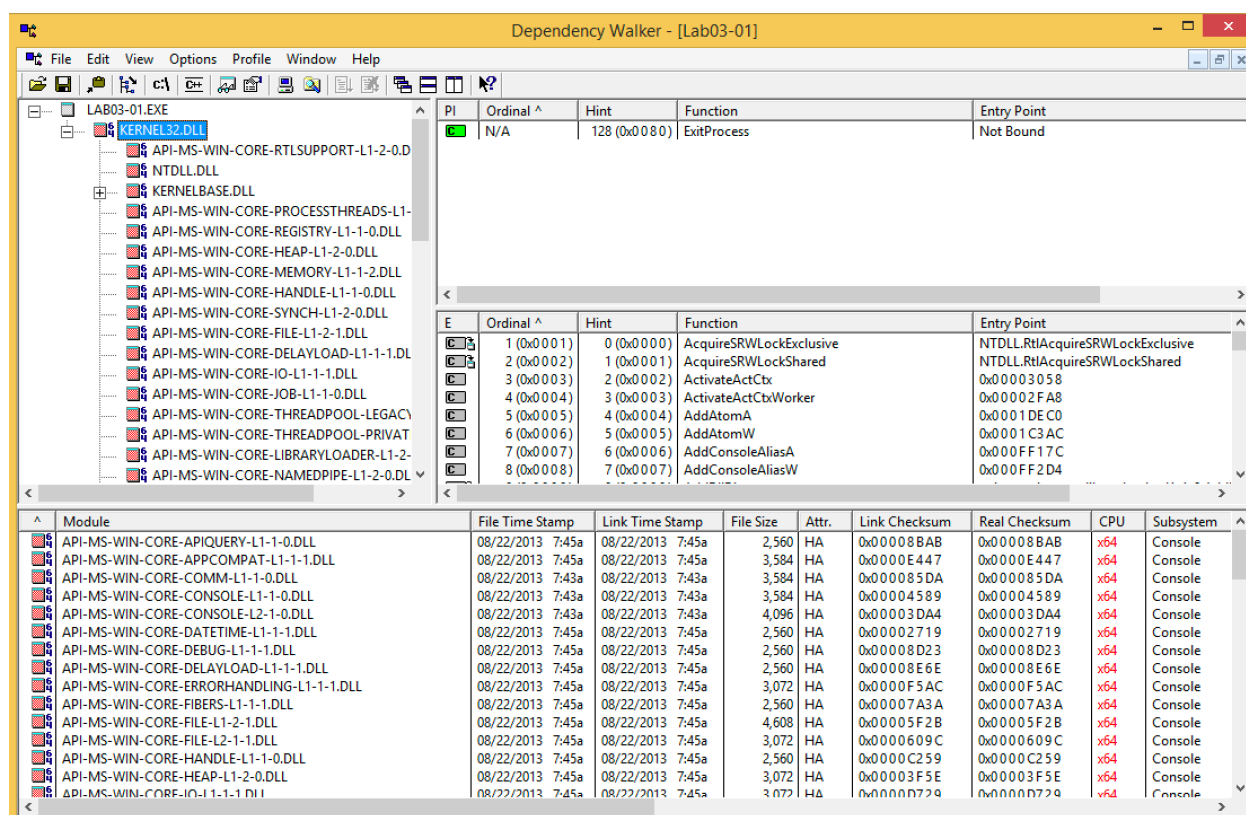
As can be seen in the above two images, a list of the DLLs used by the malware are listed. We can also see the registry keys that are opened by the malware and the different modules that are loaded.

I ran the strings command to extract every ASCII and Unicode string. This can help us determine any hardcoded IPs or domains as well as error messages. In the above images, the one on the right is a lot more interesting because we can see the registry keys hardcoded as well as a few user accounts like user32 and admin. We also see a hardcoded domain name.

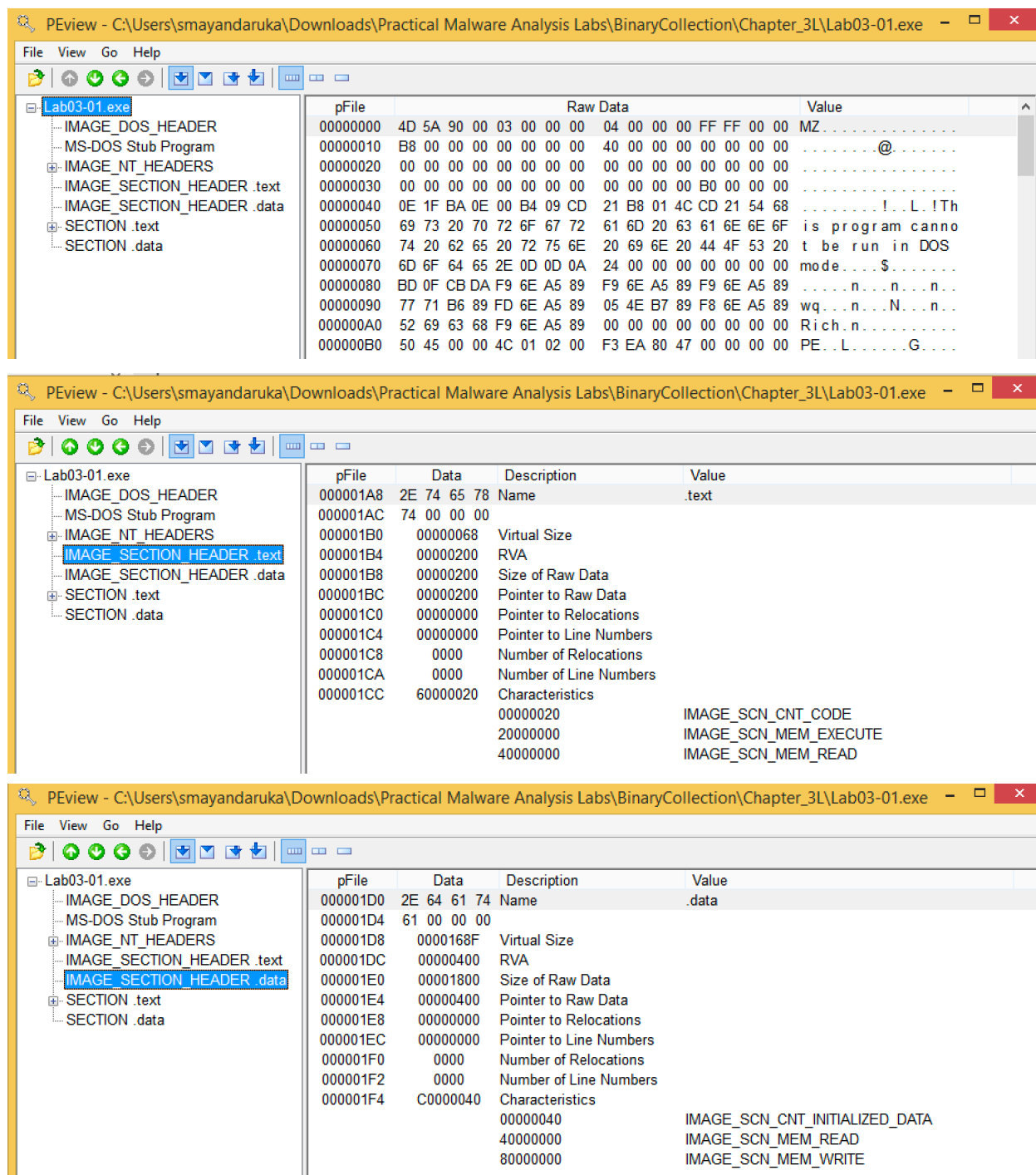
The next step was to determine whether the executable is packed or not. As can be seen in the images below, the entry point and the file offset match which indicates that this file is not packed.



I proceeded to use dependency walker to determine the dynamically linked libraries used by the executable. The image below shows the findings:



As can be seen in the above image, this executable uses the Kernel32 DLL, and we also see the rest of the dependencies. This DLL is a pretty common one since it contains core functionality, and access as well as manipulation of memory and files.



The above images show the output from PView where we can see the various sizes of the headers as well as other interesting information.

This concludes the static analysis stage. Moving forward is the dynamic analysis.

DYNAMIC TOOLS/ANALYSIS:

The first step is to use ProcMon (Process Monitor) to determine all processes activity on the system. I filtered out to look for any registry edits the executable (malware) makes on the system. The image below shows my findings:

Sequence	Time of Day	Process Name	PID	Operation	Path	Result	Detail
0	8:59:53.3208571 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 72, ...
1	8:59:53.3208992 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 1.6...
2	8:59:55.0692023 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Classes\Local Settings\Software\Microsoft\...	SUCCESS	Type: REG_BINARY, Length: 39, ...
3	8:59:55.0694305 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Classes\Local Settings\Software\Microsoft\...	SUCCESS	Type: REG_BINARY, Length: 20, ...
4	8:59:55.0697880 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Classes\Local Settings\Software\Microsoft\...	SUCCESS	Type: REG_BINARY, Length: 20, ...
5	8:59:55.0762336 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Classes\Local Settings\Software\Microsoft\...	SUCCESS	Type: REG_BINARY, Length: 39, ...
6	8:59:55.0763703 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Classes\Local Settings\Software\Microsoft\...	SUCCESS	Type: REG_BINARY, Length: 20, ...
7	8:59:55.1397392 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Classes\Local Settings\Software\Microsoft\...	SUCCESS	Type: REG_MULTI_SZ, Length: 2...
8	8:59:55.2127823 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_QWORD, Length: 8
9	8:59:55.2128460 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_DWORD, Length: 4, ...
10	8:59:55.2128556 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_SZ, Length: 520, Dat...
11	8:59:55.2173610 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_QWORD, Length: 8
12	8:59:55.2173786 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_SZ, Length: 210, Dat...
13	8:59:55.2173857 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_DWORD, Length: 4, ...
14	8:59:55.2173928 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_DWORD, Length: 4, ...
15	8:59:55.2174006 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_SZ, Length: 90, Data...
16	8:59:55.2174068 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_QWORD, Length: 8
17	8:59:55.2174129 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_QWORD, Length: 8
18	8:59:55.2174188 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_DWORD, Length: 4, ...
19	8:59:55.2174244 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_DWORD, Length: 4, ...
20	8:59:55.2174296 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_QWORD, Length: 8
21	8:59:55.2174361 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_DWORD, Length: 4, ...
22	8:59:55.2174417 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_DWORD, Length: 4, ...
23	8:59:55.2174479 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_DWORD, Length: 4, ...
24	8:59:55.2174535 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_DWORD, Length: 4, ...
25	8:59:55.2174596 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_QWORD, Length: 8
26	8:59:55.2174655 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_QWORD, Length: 8
27	8:59:55.2196219 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_QWORD, Length: 8
28	8:59:55.2196364 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_SZ, Length: 90, Data...
29	8:59:55.2274619 PM	svchost.exe	524	RegSetValue	HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppC...	SUCCESS	Type: REG_BINARY, Length: 60, ...
30	8:59:55.2282746 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 72, ...
31	8:59:55.2283089 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 1.6...
32	8:59:55.2533777 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 72, ...
33	8:59:55.2534185 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 1.6...
34	8:59:58.6205871 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 72, ...
35	8:59:58.6209121 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 1.6...
36	8:59:59.7415152 PM	svchost.exe	524	RegSetValue	HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppC...	SUCCESS	Type: REG_BINARY, Length: 108...
37	9:00:01.6138827 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 72, ...
38	9:00:01.6139689 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 1.6...

Showing 39 of 88,911 events (0.043%) Backed by virtual memory

As we can see, this executable made a lot of registry changes such as those to Microsoft registries as well as explorer and a few others.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	96.76	0 K	24 K	0		
System	0.16	28,844 K	2,320 K	4		
Interrupts	0.14	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		284 K	412 K	476		
csrss.exe	< 0.01	1,736 K	1,944 K	556		
wininit.exe		708 K	636 K	608		
services.exe		2,240 K	3,436 K	672		
svchost.exe		3,584 K	4,732 K	756	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		6,232 K	8,908 K	1296		
WWAHost.exe	Susp...	46,712 K	2,936 K	1104	Microsoft WWA Host	Microsoft Corporation
RuntimeBroker.exe		2,020 K	1,752 K	908	Runtime Broker	Microsoft Corporation
WSHost.exe		5,840 K	5,236 K	2400	Store Broker	Microsoft Corporation
svchost.exe		3,304 K	4,196 K	788	Host Process for Windows S...	Microsoft Corporation
vmacthlp.exe		968 K	800 K	972	VMware Activation Helper	VMware, Inc.
svchost.exe		12,900 K	11,912 K	992	Host Process for Windows S...	Microsoft Corporation
svchost.exe		20,012 K	24,804 K	1020	Host Process for Windows S...	Microsoft Corporation
taskhost.exe		3,800 K	4,112 K	2496	Host Process for Windows T...	Microsoft Corporation
taskeng.exe		1,048 K	4,468 K	2428		
svchost.exe		5,876 K	6,828 K	540	Host Process for Windows S...	Microsoft Corporation
svchost.exe		47,104 K	50,128 K	524	Host Process for Windows S...	Microsoft Corporation
svchost.exe		5,872 K	7,620 K	1040	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe		5,912 K	4,936 K	1160	Spooler SubSystem App	Microsoft Corporation
svchost.exe		15,256 K	14,024 K	1184	Host Process for Windows S...	Microsoft Corporation
VGAUTHSERVICE.exe		4,180 K	3,300 K	1412	VMware Guest Authentication...	VMware, Inc.
vmtoolsd.exe	0.08	7,724 K	9,536 K	1456	VMware Tools Core Service	VMware, Inc.
MsMpEng.exe	0.40	131,052 K	127,700 K	1508	Antimalware Service Execut...	Microsoft Corporation
dllhost.exe		3,124 K	2,812 K	1816	COM Surrogate	Microsoft Corporation
msdtc.exe		2,076 K	1,660 K	2020	Microsoft Distributed Transa...	Microsoft Corporation
NisSrv.exe		3,952 K	1,436 K	2060	Microsoft Network Realtime I...	Microsoft Corporation
svchost.exe		1,996 K	2,416 K	2744	Host Process for Windows S...	Microsoft Corporation
SearchIndexer.exe		20,220 K	16,532 K	2884	Microsoft Windows Search I...	Microsoft Corporation
SearchFilterHost.exe	0.02	1,004 K	4,224 K	3700		
SearchProtocolHost.e...	0.04	1,316 K	4,776 K	3948		
lsass.exe	0.09	3,392 K	4,508 K	680	Local Security Authority Proc...	Microsoft Corporation
csrss.exe	0.01	2,244 K	7,840 K	616		
winlogon.exe		1,284 K	1,652 K	688		
dwm.exe	0.12	70,288 K	86,216 K	924		
explorer.exe	0.03	82,676 K	109,860 K	2488	Windows Explorer	Microsoft Corporation
vmtoolsd.exe	0.30	12,264 K	13,272 K	2304	VMware Tools Core Service	VMware, Inc.
WzPreloader.exe	0.04	13,332 K	4,816 K	668	WinZip Preloader	WinZip Computing
chrome.exe	0.02	49,712 K	59,224 K	2584	Google Chrome	Google Inc.
chrome.exe		1,376 K	1,444 K	1056	Google Chrome	Google Inc.

CPU Usage: 3.24% Commit Charge: 28.35% Processes: 49 Physical Usage: 27.11%

As can be seen in the image on the left, Process Explorer is more or less the same as Task Manager except that it gives a lot more detail. This is really useful when performing basic dynamic analysis since it allows us to determine what new processes are run when the malware is executed.

I also ran ApatDNS but there were no entries. This is likely because there was no domain name that was resolved by the malware when it executed. I did see some local traffic which is attached below.

Time	Domain Requested	DNS Returned
21:19:23	wpad.localdomain	FOUND
21:19:23	wpad.localdomain	FOUND
21:19:24	www.google.com	FOUND
21:19:36	win8.ipv6.microsoft.com	FOUND

[+] DNS set to 127.0.0.1 on Intel(R) 82574L Gigabit Network Connection.
 [+] Sending valid DNS response of first request.
 [+] Server started at 21:19:21 successfully.
 [-] Already initiated...
 [+] Stopping Server...
 [+] DHCP detected, setting DNS back to DHCP.
 [+] DNS Restored.
 [+] Interfaces list has been refreshed.

DNS Reply IP (Default: Current Gateway/DNS):

of NXDOMAIN's:

Selected Interface:

Start Server Stop Server