

SEPparser: Symantec is Trying to Tell You Something

Brian Maloney



I am Brian Maloney

- SEPparser
- DeXRAY (McAfee/Symantec quarantine files)
- Targets/Modules for KAPE
- PCAP_tools plugin (ProcDOT)

You can find me at:

Twitter @bmmloney97

<https://github.com/Beercow>

<https://malwaremaloney.blogspot.com/>

Current State

◆ Symantec Endpoint Logs

- In TSV ish format but not human readable
- Logs have different layouts
- Some data is hidden inside VBNs (quarantine files) and ccSubSDK (submission database)
- Can only be view on live endpoint

Who can tell me what this means?

[illegible]

Current State

- ◆ Symantec Management Console
 - Only shows historical events of current user (stored in %appdata% folder)
 - Cannot view logs on another endpoint
 - Does not show all data contained in a log
 - Cannot view logs from dead box/collection

Current State

- ◆ SEP-log-conversion-macro_v2.xlsm^[1]
 - Only parses daily av logs
 - Can view logs from dead box/collection
- ◆ Log2timeline/plaso^[2]
 - Only parses daily av logs
 - Can view logs from dead box/collection
- ◆ DeXRAY^[3]
 - Extract quarantine data
 - Extract ccSubSDK database ***limited**

[1] <https://support.symantec.com/us/en/article.tech100099.html>

[2] <https://github.com/log2timeline/plaso/releases>

[3] <http://hexacorn.com/d/DeXRAY.pl>

Solution

◆ SEPparser

- Can show historical data of all users
- Can view logs on another endpoint
- Shows all data contained in a log
- View logs from dead box/collection
- View logs from other sources (VBN & ccSubSDK)
- Combine logs from different endpoints
- Platform independent

How about now?

Date and Time	Action	Sev...	Direction	Prot...	Remote ...	Remote MAC	Remote Port	Local Host	Local MAC	Local Port	Locati...	Oc...	Begin Time	End Time	Rule	
⚡	⚡	⚡	⚡	⚡	⚡	⚡	⚡	⚡	⚡	⚡	⚡	⚡	⚡	⚡	⚡	
2019-11-06 00:28:52...	Block	0	Incoming	UDP	0.0.0.0	02-0f-b5-22-11-3e	68	255.255.255.255	ff-ff-ff-ff-ff-ff	67	Default	5	2019-11-06 00:27:50...	2019-11-06 00:27:16...	Block Inbound Ma	
2019-11-06 00:32:59...	Block	0	Incoming	UDP	0.0.0.0	58-bd-a3-78-32-a5	68	255.255.255.255	ff-ff-ff-ff-ff-ff	67	Default	2	2019-11-06 00:31:55...	2019-11-06 00:30:57...	Block Inbound Ma	
2019-11-06 00:43:15...	Block	0	Incoming	UDP	0.0.0.0	58-bd-a3-78-32-a5	68	255.255.255.255	ff-ff-ff-ff-ff-ff	67	Default	2	2019-11-06 00:42:14...	2019-11-06 00:41:55...	Block Inbound Ma	
2019-11-06 00:53:00...	Block	0	Incoming	UDP	0.0.0.0	58-bd-a3-78-32-a5	68	255.255.255.255	ff-ff-ff-ff-ff-ff	67	Default	1	2019-11-06 00:51:55...	2019-11-06 00:51:55...	Block Inbound Ma	
2019-11-06 00:54:01...	Block	0	Incoming	UDP	0.0.0.0	58-bd-a3-78-32-a5	68	255.255.255.255	ff-ff-ff-ff-ff-ff	67	Default	1	2019-11-06 00:52:57...	2019-11-06 00:52:57...	Block Inbound Ma	
2019-11-06 01:02:55...	Block	0	Incoming	UDP	0.0.0.0	58-bd-a3-78-32-a5	68	255.255.255.255	ff-ff-ff-ff-ff-ff	67	Default	1	2019-11-06 01:01:55...	2019-11-06 01:01:55...	Block Inbound Ma	
2019-11-06 01:04:58...	Block	0	Incoming	UDP	0.0.0.0	58-bd-a3-78-32-a5	68	255.255.255.255	ff-ff-ff-ff-ff-ff	67	Default	1	2019-11-06 01:03:55...	2019-11-06 01:03:55...	Block Inbound Ma	
2019-11-06 01:13:00...	Block	0	Incoming	UDP	0.0.0.0	58-bd-a3-78-32-a5	68	255.255.255.255	ff-ff-ff-ff-ff-ff	67	Default	1	2019-11-06 01:11:57...	2019-11-06 01:11:57...	Block Inbound Ma	
2019-11-06 01:16:00...	Block	0	Incoming	UDP	0.0.0.0	58-bd-a3-78-32-a5	68	255.255.255.255	ff-ff-ff-ff-ff-ff	67	Default	1	2019-11-06 01:14:57...	2019-11-06 01:14:57...	Block Inbound Ma	
2019-11-06 01:22:56...	Block	0	Incoming	UDP	0.0.0.0	58-bd-a3-78-32-a5	68	255.255.255.255	ff-ff-ff-ff-ff-ff	67	Default	1	2019-11-06 01:21:55...	2019-11-06 01:21:55...	Block Inbound Ma	
2019-11-06 01:26:57...	Block	0	Incoming	UDP	0.0.0.0	58-bd-a3-78-32-a5	68	255.255.255.255	ff-ff-ff-ff-ff-ff	67	Default	1	2019-11-06 01:25:55...	2019-11-06 01:25:55...	Block Inbound Ma	
2019-11-06 01:32:56...	Block	0	Incoming	UDP	0.0.0.0	58-bd-a3-78-32-a5	68	255.255.255.255	ff-ff-ff-ff-ff-ff	67	Default	1	2019-11-06 01:31:55...	2019-11-06 01:31:55...	Block Inbound Ma	
LOG:Time(UTC)	LOG:Event				LOG:Category	LOG:Logger	LOG:Com...	LOG:User	LOG:Virus	LOG:File		LOG:Wanted...	LOG:Wa...	LOG:Real A...	LOG:Virus_Type	LOG:Flags
⚡	⚡				⚡	⚡	⚡	⚡	⚡	⚡		⚡	⚡	⚡	⚡	⚡
2019-08-29 19:16:54	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:16:54	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:27:43	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:16:54	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:27:43	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:16:54	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:27:43	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:16:54	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:27:43	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:16:54	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:27:43	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:16:54	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:27:43	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:54:13	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:54:13	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:54:13	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:54:13	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:54:13	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:54:13	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-29 19:54:13	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-30 19:15:48	ANOMALY_START				Infection	Real_Time	*****...	SYSTEM	PasswordRevealer!g1	C:\Program Files (x86)\...	Quarantine	Delete	Quarantine	Reputation	EB_REAL_CLIENT F	
2019-08-30 19:15:49	ANOMALY_FINISH				Infection	Real_Time	*****...	SYSTEM	PasswordRevealer!g1	C:\Program Files (x86)\...	Quarantine	Delete	Quarantine	Reputation	EB_ACCESS_DENIED	
2019-08-30 19:15:48	INFECTION				Infection	Real_Time	*****...	SYSTEM	PasswordRevealer!g1	C:\Program Files (x86)\...	Quarantine	Delete	Quarantine	Reputation	EB_ACCESS_DENIED	
2019-08-30 19:16:37	ANOMALY_START				Infection	Real_Time	*****...	SYSTEM	HackTool.Produkey	C:\Program Files (x86)\...	Quarantine	Delete	Quarantine	Hack Tools	EB_REAL_CLIENT F	
2019-08-30 19:16:37	ANOMALY_FINISH				Infection	Real_Time	*****...	SYSTEM	HackTool.Produkey	C:\Program Files (x86)\...	Quarantine	Delete	Quarantine	Hack Tools	EB_ACCESS_DENIED	
2019-08-30 19:16:37	INFECTION				Infection	Real_Time	*****...	SYSTEM	Hacktool.ProduKey	C:\Program Files (x86)\...	Quarantine	Delete	Quarantine	Hack Tools	EB_ACCESS_DENIED	
2019-08-30 19:27:03	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								
2019-08-30 19:27:03	SECURITY_SYMPROTECT_POLICYVIOLATION				Security	SymProtect	*****...	SYSTEM								

1. Symantec Logs

Locations and types

Symantec Logs

- ◆ C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Logs contain the following log files:
 - AVMan.log - Antivirus Management plug-in log (contains copies of all antivirus events)
 - CVE.log Client communication logs (14.2 and up)
 - CVE-actions.log Client communications actions (14.2 and up)
 - GUPProxy.log - GUP plug-in log (if you have a GUP enabled)
 - LUMan.log - Symantec Endpoint Protection (SEP) Client LiveUpdate plug-in log
 - processlog.log - Application and Device Control log
 - rawlog.log - Firewall Packet log
 - seclog.log - Security log (IPS events mainly)
 - syslog.log - System log
 - tralog.log - Firewall Traffic log

<https://support.symantec.com/us/en/article.tech141236.html>

Symantec Logs Continued

C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Logs\AV

- Contains daily antivirus logs

%LOCALAPPDATA%\Symantec\Symantec Endpoint Protection\Logs

- Contains daily antivirus logs

C:\ProgramData\Symantec\Symantec\Endpoint Protection\CurrentVersion\Data\Quarantine

- VBN files contain a log line also

C:\ProgramData\Symantec\Symantec\Endpoint Protection\CurrentVersion\Data\CmnClnt\ccSubSDK

- ccSubSDK database includes information about antivirus detections, intrusion prevention, SONAR, and file reputation detections

Which log is which?

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\smc -exportlog

Exports the entire contents of a log to a .txt file.

To export a log, you use the following syntax:

smc -exportlog log_type 0 -1 output_file

where:

log_type is:

- 0 = System Log
- 1 = Security Log
- 2 = Traffic Log
- 3 = Packet Log
- 4 = Control Log

Which log is which?

◆ These numbers also correlate to an entry in the header of the log file

- 0 = syslog.log
- 1 = seclog.log
- 2 = tralog.log
- 3 = rawlog.log
- 4 = processlog.log

00000002	00400000	0000017a	00001e30	000016f9	000000000003662d	0000000e
Log Type	Log Size		# of Logs			# of Days

2.

Network and Host Exploit Mitigation Packet Log

Firewall Packet Log

SMC GUI shows packet data

Packet Log - Network and Host Exploit Mitigation Logs

File Edit View Filter Action Help

Date and Time	Remote Host	Remote Port	Local Host	Local ...	Direction	Action	Application
12/16/2019 1:10:17 PM	192.168.0.3	58222	192.168.0.2	3389	Incoming	Blocked	C:\Windows\System32\svchost.exe
12/16/2019 1:10:09 PM	192.168.0.3	58222	192.168.0.2	3389	Incoming	Blocked	C:\Windows\System32\svchost.exe
12/16/2019 1:10:05 PM	192.168.0.3	58222	192.168.0.2	3389	Incoming	Blocked	C:\Windows\System32\svchost.exe
12/16/2019 1:10:02 PM	192.168.0.3	58222	192.168.0.2	3389	Incoming	Blocked	C:\Windows\System32\svchost.exe
12/16/2019 1:10:01 PM	192.168.0.3	58222	192.168.0.2	3389	Incoming	Blocked	C:\Windows\System32\svchost.exe

Ethernet II (Packet Length: 66)

Destination: 00-24-9b-44-00-57

Source: e0-cb-4e-31-bd-80

Type: IP (0x800)

Internet Protocol

Version: 4

Header Length: 20 bytes

Flags:

.1.. = Don't fragment: Set

..0. = More fragments: Not set

Fragment offset:0

Time to live: 128

Protocol: 0x6

Header checksum: 0xe7fe (Correct)

(TCP - Transmission Control Protocol)

Source: 192.168.0.3

Destination: 192.168.0.2

Transmission Control Protocol (TCP)

Source port: 58222

Destination port: 3389

Sequence number: 982613866

Acknowledgment number: 0

Header length: 32

Flags:

0000: 00 24 9B 44 00 57 E0 CB : 4E 31 BD 80 08 00 45 00 | .\$.D.W..Nl....E.

0010: 00 34 91 6F 40 00 80 06 : E7 FE C0 A8 00 03 C0 A8 | .4.o@.....

0020: 00 02 E3 6E 0D 3D 3A 91 : 7F 6A 00 00 00 00 80 02 | ...n.=:...j.....

0030: FA F0 48 22 00 00 02 04 : 05 B4 01 03 03 08 01 01 | ..H".....

0040: 04 02 : | ..

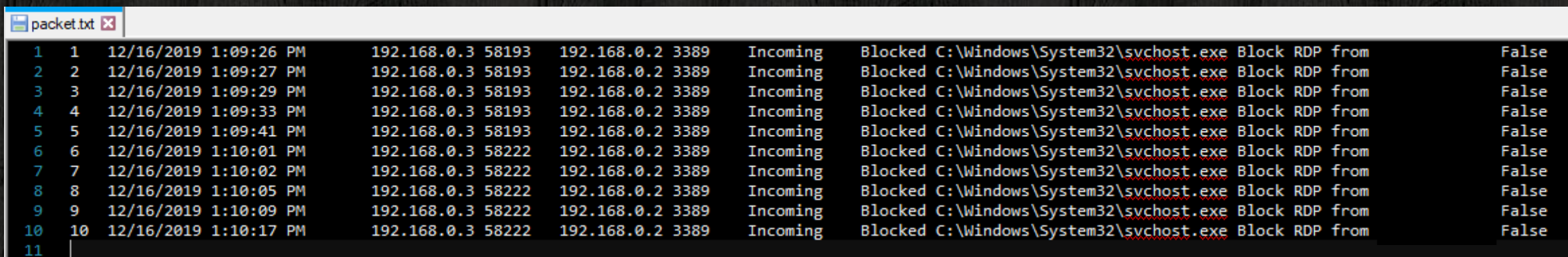
Current log file size: 3 KB, Maximum size: 1,024 KB

Records: 10

Filter: 1 day

Network and Host Exploit Mitigation Packet Log

- ◆ Can dump log via command line
 - *c:\Program Files (x86)\Symantec\Symantec Endpoint Protection\Smc.exe" -exportlog 3 0 -1 c:\temp\packet.txt*
- ◆ No packet data
- ◆ But what about dead box/collection?



1	1	12/16/2019 1:09:26 PM	192.168.0.3	58193	192.168.0.2	3389	Incoming	Blocked	C:\Windows\System32\svchost.exe	Block	RDP	from	False
2	2	12/16/2019 1:09:27 PM	192.168.0.3	58193	192.168.0.2	3389	Incoming	Blocked	C:\Windows\System32\svchost.exe	Block	RDP	from	False
3	3	12/16/2019 1:09:29 PM	192.168.0.3	58193	192.168.0.2	3389	Incoming	Blocked	C:\Windows\System32\svchost.exe	Block	RDP	from	False
4	4	12/16/2019 1:09:33 PM	192.168.0.3	58193	192.168.0.2	3389	Incoming	Blocked	C:\Windows\System32\svchost.exe	Block	RDP	from	False
5	5	12/16/2019 1:09:41 PM	192.168.0.3	58193	192.168.0.2	3389	Incoming	Blocked	C:\Windows\System32\svchost.exe	Block	RDP	from	False
6	6	12/16/2019 1:10:01 PM	192.168.0.3	58222	192.168.0.2	3389	Incoming	Blocked	C:\Windows\System32\svchost.exe	Block	RDP	from	False
7	7	12/16/2019 1:10:02 PM	192.168.0.3	58222	192.168.0.2	3389	Incoming	Blocked	C:\Windows\System32\svchost.exe	Block	RDP	from	False
8	8	12/16/2019 1:10:05 PM	192.168.0.3	58222	192.168.0.2	3389	Incoming	Blocked	C:\Windows\System32\svchost.exe	Block	RDP	from	False
9	9	12/16/2019 1:10:09 PM	192.168.0.3	58222	192.168.0.2	3389	Incoming	Blocked	C:\Windows\System32\svchost.exe	Block	RDP	from	False
10	10	12/16/2019 1:10:17 PM	192.168.0.3	58222	192.168.0.2	3389	Incoming	Blocked	C:\Windows\System32\svchost.exe	Block	RDP	from	False
11													

Network and Host Exploit Mitigation Packet Log

- ◆ SEPparser gives you the same data as SMC GUI
- ◆ Also places packets into separate file

Date and Time	Remote Host	Remote Port	Local Host	Local Port	Directi...	Action	Application	Packet Dump	Packet Decode
2019-12-16 19:09:26.878388	192.168.0.3	58193	192.168.0.2	3389			C:\Windows\System32\svchost.exe		000000 00 24 9b 44 00 57 e0 cb 4e 31 bd 80 08 00 45 00 .\$.D
2019-12-16 19:09:27.884650	192.168.0.3	58193	192.168.0.2	3389			C:\Windows\System32\svchost.exe		000000 00 24 9b 44 00 57 e0 cb 4e 31 bd 80 08 00 45 00 .\$.D
2019-12-16 19:09:29.804160	192.168.0.3	58193	192.168.0.2	3389			C:\Windows\System32\svchost.exe		000000 00 000000 00 24 9b 44 00 57 e0 cb 4e 31 bd 80 08 00 45 00 .\$.D
2019-12-16 19:09:33.830034	192.168.0.3	58193	192.168.0.2	3389			C:\Windows\System32\svchost.exe		000000 00 000010 00 34 91 66 40 00 80 06 e8 07 c0 a8 00 03 c0 a8 .4.f@.....
2019-12-16 19:09:41.875962	192.168.0.3	58193	192.168.0.2	3389			C:\Windows\System32\svchost.exe		000000 00 000020 00 02 e3 51 0d 3d d2 d5 f6 55 00 00 00 80 02 ...Q.=...U.....
2019-12-16 19:10:01.991526	192.168.0.3	58222	192.168.0.2	3389			C:\Windows\System32\svchost.exe		000000 00 000030 fa f0 39 0f 00 00 02 04 05 b4 01 03 03 08 01 01 ..9.....
2019-12-16 19:10:02.998484	192.168.0.3	58222	192.168.0.2	3389			C:\Windows\System32\svchost.exe		000000 00 000040 04 02 ..
2019-12-16 19:10:05.008124	192.168.0.3	58222	192.168.0.2	3389			C:\Windows\System32\svchost.exe		000000 00
2019-12-16 19:10:09.030546	192.168.0.3	58222	192.168.0.2	3389			C:\Windows\System32\svchost.exe		000000 00
2019-12-16 19:10:17.078878	192.168.0.3	58222	192.168.0.2	3389			C:\Windows\System32\svchost.exe		000000 00

packet.txt

Symantec_Client_Management_Control_Log.csv

Symantec_Client_Management_Security_Log.csv

Symantec_Client_Management_System_Log.csv

Symantec_Client_Management_Tamper_Protect_Log.csv

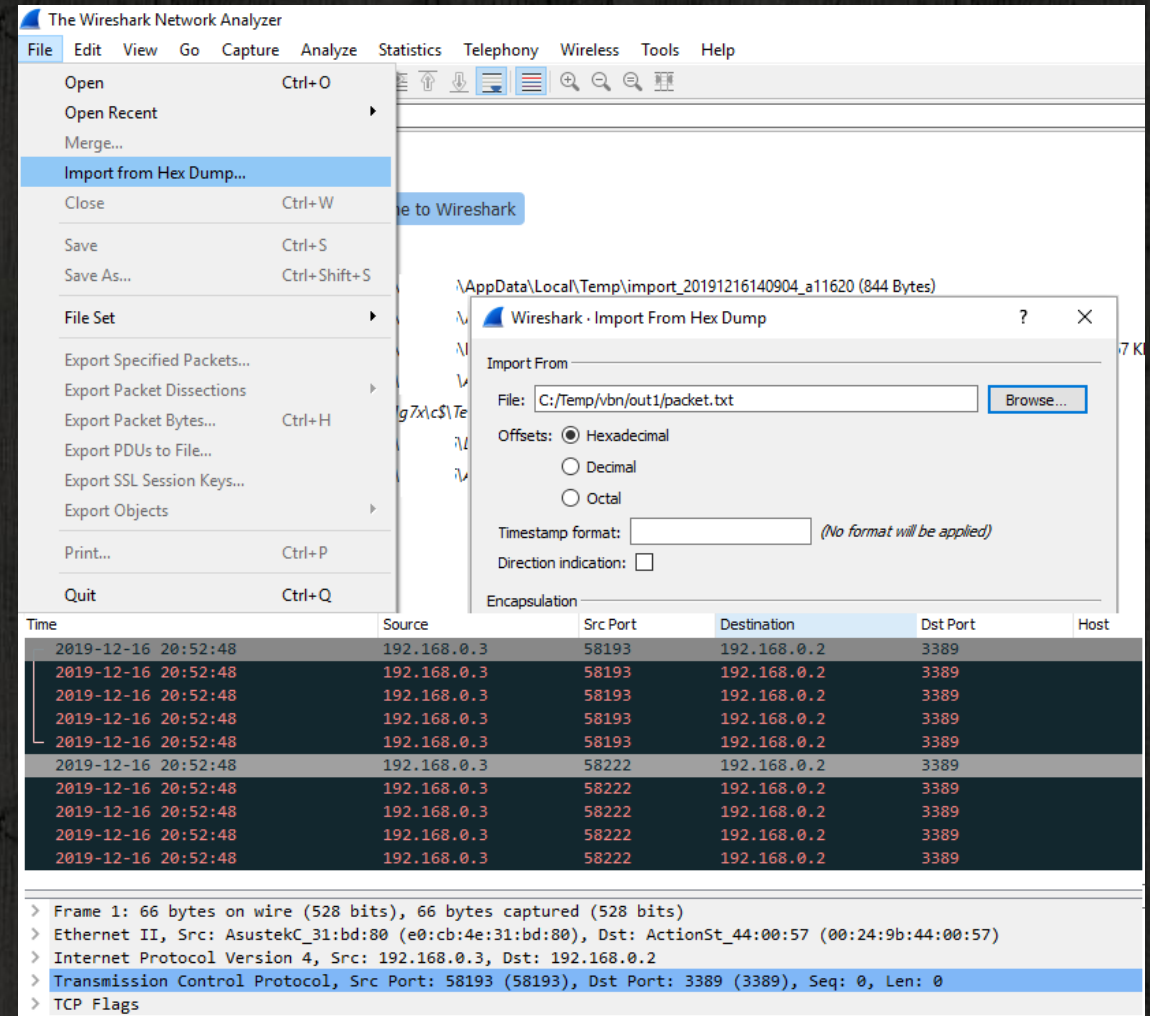
Symantec_Network_and_Host_Exploit_Mitigation_Packet_Log.csv

Symantec_Network_and_Host_Exploit_Mitigation_Traffic_Log.csv

Symantec_Timeline.csv

Network and Host Exploit Mitigation Packet Log

- ◆ Import packet.txt into Wireshark and view all the data



3. Tamper Protect Log


Symantec Access Events

Client Management Tamper Protect Log

- ◆ Subset of AVMan.log
 - Alerts on access to Symantec Components
 - Data distinct enough to justify its own log

Client Management Tamper Protect Log

- ◆ SMC shows 1 event
- ◆ There were 304 events in the log

Tamper Protection Log								
Computer	User	Action Tak...	Object Type	Event	Actor	Target	Target Process	Date and Time
		Blocked	File	Create	C:\WINDOWS\EXPLORER.EXE (PID 10668)	C:\ProgramData\Symantec\Symantec Endpoint Protection\14.2.1031.0100.105\Data\Logs\rawlog.log	(PID 0)	12/12/2019 1:05:01 PM

File	Create	C:\WINDOWS\EXPLORER.EXE (PID 10668)	C:\ProgramData\Symantec\Symantec Endpoint Protection\14.2.1031.0100.105\Data\Logs\rawlog.log	(PID 0)	2019-12-12 19:05:01
File	Create	C:\WINDOWS\SYSTEM32\DLLHOST.EXE (PID 5896)	C:\ProgramData\Symantec\Symantec Endpoint Protection\14.2.1031.0100.105\Data\Logs\rawlog.log	(PID 0)	2019-12-12 19:05:13
File	Create	C:\WINDOWS\CMD.EXE (PID 17148)	C:\ProgramData\Symantec\Symantec Endpoint Protection\14.2.1031.0100.105\Data\Logs\rawlog.log	(PID 0)	2019-12-12 19:10:12
File	Create	C:\WINDOWS\SYSTEM32\CMD.EXE (PID 4060)	C:\ProgramData\Symantec\Symantec Endpoint Protection\14.2.1031.0100.105\Data\Logs\rawlog.log	(PID 0)	2019-12-12 19:12:10
File	Create	C:\WINDOWS\EXPLORER.EXE (PID 10668)	C:\ProgramData\Symantec\Symantec Endpoint Protection\14.2.1031.0100.105\Data\Logs\rawlog.log	(PID 0)	2019-12-12 19:05:01
File	Create	C:\WINDOWS\SYSTEM32\DLLHOST.EXE (PID 5896)	C:\ProgramData\Symantec\Symantec Endpoint Protection\14.2.1031.0100.105\Data\Logs\rawlog.log	(PID 0)	2019-12-12 19:05:13
File	Create	C:\WINDOWS\CMD.EXE (PID 17148)	C:\ProgramData\Symantec\Symantec Endpoint Protection\14.2.1031.0100.105\Data\Logs\rawlog.log	(PID 0)	2019-12-12 19:10:12
File	Create	C:\WINDOWS\SYSTEM32\CMD.EXE (PID 4060)	C:\ProgramData\Symantec\Symantec Endpoint Protection\14.2.1031.0100.105\Data\Logs\rawlog.log	(PID 0)	2019-12-12 19:12:10

4.

Virus and Spyware Protection Risk Log

Virus and Spyware Protection Risk Log

◆ Files, registry setting etc.. that are deemed suspicious/malicious

The screenshot displays the Symantec Endpoint Protection interface. The 'View Logs - Symantec Endpoint Protection' window is open, showing the 'Virus and Spyware Protection Logs' tab. The 'Risk Log' is selected, displaying a table of risk events. One entry for 'TimelineExplorer.exe' is highlighted, showing a 'Manual Submission' action with a 'Restart Required' risk.

Filename	Risk	Action	Risk Type	Logged By
hindsight_gui.exe	WS.Reputation.1	Log only	Insight Networ...	Auto-Protect s...
TimelineExplorer.exe	Manual Submi...	Restart Re...	Virus	Manual Quara...
TimelineExplorer.exe	Manual Submi...	Restart Re...	Virus	Manual Quara...
TimelineExplorer.exe	Manual Submi...	Restart Re...	Virus	Manual Quara...

The 'Risk Details' window for the selected entry is also visible, titled 'Manual Submission'. It provides detailed information about the file, including its action description, date found, category, and various reputation and prevalence metrics.

Action description: Restart Required - The file was quarantined suc

Date found: 11/8/2019

Category: Malware

Sub category: Virus

Download site: Not available

Downloaded by: c:\windows\explorer.exe

Source Computer: Local host

File size: 58890616

Company name: Eric R. Zimmerman

Product version: 0.9.5.0

Hash: 90DE486D6285A2E216BC2B048CA9A3C8CE9 56193F7ED6ED22CCFD3F43BF1A663

Current location: Quarantine

Status: Clean

Scan type: Manual Quarantine Scan

SONAR Risk level: Not available

SONAR Confidence level: Not available

Historical Reputation: Symantec Endpoint Protection believes this file

Historical Prevalence: This file has been seen by fewer than 5 Syman

First Seen: Symantec has known about this file approximal

Current Reputation: Symantec Endpoint Protection believes this file

Current Prevalence: This file has been seen by fewer than 50 Syma

URL Tracking: On

Corrective Actions:

Type	Description	Action Taken	Remediation Status
File	C:\Users\ Downloads\TimelineE...	Quarantine	Successful - Restart...
Browser Ca...	Internet browser temporary file cache	Deleted	Successful

Virus and Spyware Protection Risk Log

File Name	Digital_Signatures_Signer	Digital_Signatures_Issuer	Digital_Signatures_Certificate_Thumbprint	Digital_Signatures_Serial_Number	Digital_Signatures_Signing_Time
Logs\AVMan.log	Eric R. Zimmerman	COMODO RSA Code Signing CA	E6D61D0F1F587F44C8B5734519B6AF742D3C57A1	2421252F033C2EA94AA97B893E0ED780	2019-11-05 16:02:52
Logs\AVMan.log	Eric R. Zimmerman	COMODO RSA Code Signing CA	E6D61D0F1F587F44C8B5734519B6AF742D3C57A1	2421252F033C2EA94AA97B893E0ED780	2019-11-05 16:02:52
Logs\Quarantine\0CA40000.VBN					
Logs\Quarantine\4CB80000.VBN					
Logs\Quarantine\0CA40000\5DE59F6B.VBN					
Logs\Quarantine\4CB80000\5DFD896A.VBN					
Logs\Quarantine\Restored\4CB80000.VBN					
Logs\Quarantine\Restored\4CB80000\5D...					

```

1  X509 Certificate:
2  Version: 3
3  Serial Number: 2421252f033c2ea94aa97b893e0ed780
4  Signature Algorithm:
5    Algorithm ObjectID: 1.2.840.113549.1.1.11 sha256RSA
6    Algorithm Parameters:
7      05 00
8  Issuer:
9  CN=COMODO RSA Code Signing CA
10 O=COMODO CA Limited
11 L=Salford
12 S=Greater Manchester
13 C=GB
14 Name Hash(sha1): 927715dd1b8e3bca691134f5558942efdeb901c
15 Name Hash(md5): 257de1d254502d00acd30d8ea1041373
16
17 NotBefore: 1/23/2017 6:00 PM
18 NotAfter: 1/24/2020 5:59 PM
19
20 Subject:
21 CN=Eric R. Zimmerman
22 00f0 78 d1 f6 be 26 f0 c9 f9 a8 16 7d 56 0d 1b fb 0d
130 Non-root Certificate
131 Key Id Hash(rfc-sha1): c53bd17386ced98e652c42cd3d565e270cb72b42
132 Key Id Hash(sha1): 7d202b11299599538cd1904ac6205f83b633f29a
133 Key Id Hash(bcrypt-sha1): e023c35f67291c47d34eddb1dc27adba5473c445
134 Key Id Hash(bcrypt-sha256): 71b3bbe7e703f0feb61ee45cdb13c02af656685aeb38a34b647dec0db872207
135 Key Id Hash(md5): 58c226ee743ffb1de0115a2b25a78f4d
136 Key Id Hash(sha256): 2257c2b8428a2e18649c2d973e6336a2454774d551654c55945e430f9c3e41bf
137 Key Id Hash(pin-sha256): eAvN214+XBKEPOU96wLAY7U0XQ9tLRF58ZhpkiDKM=
138 Key Id Hash(pin-sha256-hex): 780bcd5a5e3e5c12843ce53deb094063b5345d0f6d2d17f9b198699087220ca3
139 Cert Hash(md5): f4a37ca96537c13cc1bc3fb0635f8da5
140 Cert Hash(sha1): e6d61d0f1f587f44c8b5734519b6af742d3c57a1
141 Cert Hash(sha256): d0382b027e27e8e991a9a2ca01f95cb9e88e84e59458db9b3bea218ada256704
142 Signature Hash: 574e164d9812e4e069ca18788f851a95448dfb164d675f05ec67f535fdd83c3
143 CertUtil: -dump command completed successfully.
144
145

```

Digital Signature Details

General

Advanced

Digital Signature Information

This digital signature is OK.

Signer information

Name: Eric R. Zimmerman

E-mail: eric@mikestammer.com

Signing time: Tuesday, November 5, 2019 10:02:52 AM

View Certificate

Countersignatures

Name of signer: Sectigo RSA Tim...

E-mail address: Not available

Timestamp: Tuesday, November ...

Details

OK

5. VBN files

Symantec quarantine files



VBNs files

- ◆ Three different types of VBN files
 - 0x0 = Hybrid
 - 0x1 = Meta
 - 0x2 = Quarantine
- ◆ Usually an inner and outer VBN file

Name	Date created	Date accessed	Date modified	Type	Size
0CA40000	12/9/2019 9:35 AM	12/9/2019 9:35 AM	12/9/2019 9:35 AM	File folder	
4CB80000	12/9/2019 9:35 AM	12/9/2019 9:35 AM	12/9/2019 9:35 AM	File folder	
0CA40000.VBN	12/9/2019 9:35 AM	12/9/2019 9:35 AM	11/8/2019 11:01 AM	VBN File	7 KB
4CB80000.VBN	12/9/2019 9:35 AM	12/9/2019 9:35 AM	11/8/2019 9:27 AM	VBN File	7 KB

VBN Time Stamps

◆ File time stamps are also recorded in VBN

Name	Date created	Date accessed	Date modified	Type	Size
 TimelineExplorer	11/8/2019 8:54 AM	11/8/2019 11:00 AM	11/8/2019 11:00 AM	File folder	
 TimelineExplorer.exe	11/5/2019 11:02 AM	11/8/2019 11:00 AM	11/8/2019 10:59 AM	Application	57,511 KB

VBN Time Stamps

```
typedef struct VBN_METADATA {
    int32 QMF_HEADER_Offset;
    char FQP_of_Quarantine_File[384];
    char Log_line[2048];
    int32 Data_Type;
    long Record_ID;
    char Unknown1[28];
    char Unknown2[484];
    char Storage_Name[48];
    uint32 RemediationInfo.tmp_Path_Size;
    char RemediationInfo.tmp_Path[384];
    int32 Unknown3;
    int32 Unknown4;
    char Unknown5[12];
    int32 Quarantine_File_Size;
    int64 Date_Accessed;
    int64 Date_Modified;
    int64 Date_Created;
    int64 Date_Quarantined;
    char Unknown6[20];
    char Unknown7[260];
    int64 Folder_Header;
    int32 Folder_Name;
    char Unknown8[32];
    wchar FQP_of_Quarantine_File2[768 / 2];
    char Unknown9[212];
} VBN_METADATA;
```

00000d30	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000d40	02 00 00 00 00 00 ff 81	01 00 00 00 00 00 00 00
00000d50	02 00 00 00 78 99 82 03	43 9f c5 5d 00 00 00 00
00000d60	d9 9e c5 5d 00 00 00 00	40 ab c1 5d 00 00 00 00
00000d70	6b 9f c5 5d 00 00 00 00	00 00 00 00 00 00 00 00
00000d80	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000d90	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00

```
- Unknown5: '\x01\x00\x00\x00\x00\x00'
- Quarantine_File_Size: 0x3829978
- Date_Accessed: 0x5dc59f43
- Date_Modified: 0x5dc59ed9
- Date_Created: 0x5dc1ab40
- Date_Quarantined: 0x5dc59f06
- Unknown6: '\x00\x00\x00\x00\x00\x00'
```

Value to Decode: 5dc59f43

~~Date & Time:~~ **Fri, 08 November 2019 11:00:51 -0600**

Value to Decode: 5dc59ed9

Date & Time: **Fri, 08 November 2019 10:59:05 -0600**

www.digital-detective.co.uk

Value to Decode: 5dc1ab40

Date & Time: **Tue, 05 November 2019 11:02:56 -0600**

www.digital-detective.co.uk

Value to Decode: 5dc59f6b
Date & Time: **Fri, 08 November 2019 11:01:31 -0600**

www.digital-detective.co.uk

Security Descriptor Definition Language (SDDL)

00000200	6c 00 69 00 6e 00 65 00 45 00 78 00 70 00 6c 00	l.i.n.e.E.x.p.l.
00000210	6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00	o.r.e.r...e.x.e.
00000220	00 00 03 23 00 00 00 01 11 09 10 00 00 00 21 a3	...#.....!.
00000230	05 3f b7 43 78 45 93 c8 cd c5 f6 4a 14 9a 09 27	.?.CxE.....J...'
00000240	01 00 00 06 01 00 00 00 06 02 00 00 00 08 18 01
00000250	00 00 4f 00 3a 00 53 00 2d 00 31 00 2d 00 35 00	..0.:.S.-.1.-.5.
00000260	2d 00 32 00 31 00 2d 00 32 00 39 00 33 00 35 00	-.2.1.-.2.9.3.5.
00000270	30 00 31 00 37 00 31 00 34 00 36 00 2d 00 31 00	0.1.7.1.4.6.-.1.
00000280	31 00 37 00 35 00 30 00 37 00 32 00 38 00 30 00	1.7.5.0.7.2.8.0.
00000290	33 00 2d 00 33 00 36 00 30 00 36 00 34 00 37 00	3.-.3.6.0.6.4.7.
000002a0	38 00 31 00 36 00 37 00 2d 00 31 00 38 00 33 00	8.1.6.7.-.1.8.3.
000002b0	38 00 36 00 37 00 47 00 3a 00 44 00 55 00 44 00	8.6.7.G.:.D.U.D.
000002c0	3a 00 50 00 28 00 41 00 3b 00 3b 00 46 00 41 00	:.P.(.A.;.;.F.A.
000002d0	3b 00 3b 00 3b 00 53 00 59 00 29 00 28 00 41 00	;.;.;.S.Y.).(.A.
000002e0	3b 00 3b 00 46 00 41 00 3b 00 3b 00 3b 00 42 00	;.;.F.A.;.;.;.B.
000002f0	41 00 29 00 28 00 41 00 3b 00 3b 00 46 00 41 00	A.).(.A.;.;.F.A.
00000300	3b 00 3b 00 3b 00 53 00 2d 00 31 00 2d 00 35 00	;.;.;.S.-.1.-.5.
00000310	2d 00 32 00 31 00 2d 00 32 00 39 00 33 00 35 00	-.2.1.-.2.9.3.5.
00000320	30 00 31 00 37 00 31 00 34 00 36 00 2d 00 31 00	0.1.7.1.4.6.-.1.
00000330	31 00 37 00 35 00 30 00 37 00 32 00 38 00 30 00	1.7.5.0.7.2.8.0.
00000340	33 00 2d 00 33 00 36 00 30 00 36 00 34 00 37 00	3.-.3.6.0.6.4.7.
00000350	38 00 31 00 36 00 37 00 2d 00 31 00 38 00 33 00	8.1.6.7.-.1.8.3.
00000360	38 00 36 00 37 00 29 00 00 00	8.6.7.)...

Attribute Data

```
00000000  07 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  .....@.....
00000010  00 00 00 00 d4 eb c6 30 4c 76 e8 11 a4 77 00 24  .......0Lv...w.$
00000020  9b 20 b7 5f 9c cb 6b 72 2c 54 72 4b b4 48 46 93  ._. ...kr,TrK.HF.
00000030  35 23 79 be d4 eb c6 30 4c 76 e8 11 a4 77 00 24  5#y. ....0Lv...w.$
00000040  9b 20 b7 5f 00 00 00 00 00 00 00 00 00 00 00 00  . . . . .
00000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....

struct _OBJECT_ID_Attribute:
- Attribute_Type: 0x7
- Attribute_Size: 0x40
- Attribute_Name_Size: 0x0
- GUID_Object_Id: b'\xd4\xeb\xc6Lv\xe8\x11\xa4w\x00$\x9b \xb7_'
- GUID_Birth_Volume_Id: b'\x9c\xcbkr,TrK\xb4HF\x935#y\xbe'
- GUID_Birth_Object_Id: b'\xd4\xeb\xc6Lv\xe8\x11\xa4w\x00$\x9b \xb7_'
- GUID_Domain_Id: b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
Finished parsing vbn\Quarantine\20400000\7B4BDB4B.VBN
```

Cell contents

MAC Address: 00:24:9b:20:b7:5f

MAC Vendor: Action Star Enterprise Co., Ltd.

Creation: 2018-06-22 18:43:44.273506

Object ID: 30c6ebd4-764c-11e8-a477-00249b20b75f

Birth Volume ID: 726bcb9c-542c-4b72-b448-4693352379be

Birth Object ID: 30c6ebd4-764c-11e8-a477-00249b20b75f

Domain ID: 00000000-0000-0000-0000-000000000000

Detection Digest

Detection Digest:

```
03 00 EA AF 32 01 00 04 00 00 00 00 00 00 00 .....2.....
00 00 00 00 00 00 00 00 00 00 00 00 00 04 03 00 .....
00 00 00 03 06 00 01 02 04 00 01 00 05 17 00 43 .....C
3A 5C 57 69 6E 64 6F 77 73 5C 65 78 70 6C 6F 72 :\Windows\explor
65 72 2E 65 78 65 06 E4 0A 08 01 12 04 00 00 00 er.exe.....
00 1A 04 00 00 00 00 22 08 00 00 00 00 00 00 00 .....".
00 2A 08 00 00 00 00 00 00 00 00 32 A9 0D 45 53 .*.....2..ES
55 42 02 A9 06 00 00 31 00 00 00 01 00 00 00 00 UB.....1.....
00 00 00 23 00 4A 45 53 45 5F 45 4D 4F 54 45 54 ...#.JESE_EMOTET
5F 53 48 41 50 45 53 5F 54 45 58 54 5F 53 48 41 _SHAPES_TEXT_SHA
44 4F 57 5F 42 41 49 54 6F 06 00 00 00 00 41 74 DOW_BAIto.....At
74 72 69 62 75 74 65 20 56 42 5F 4E 61 6D 65 20 tribute VB_Name
3D 20 22 65 35 37 38 64 36 35 39 22 0D 0A 46 75 = "e578d659"..Fu
6E 63 74 69 6F 6E 20 65 34 62 31 62 34 62 36 28 nction e4b1b4b6(
29 0D 0A 65 34 62 31 62 34 62 36 20 3D 20 22 63 )..e4b1b4b6 = "c
3A 5C 70 72 6F 67 72 61 6D 64 61 74 61 5C 70 72 :\programdata\pr
65 76 69 65 77 2E 6A 70 65 67 22 0D 0A 45 6E 64 eview.jpeg"..End
20 46 75 6E 63 74 69 6F 6E 0D 0A 53 75 62 20 63 Function..Sub c
35 36 31 36 65 38 62 28 29 0D 0A 45 6E 64 20 53 5616e8b()..End S
75 62 0D 0A 46 75 6E 63 74 69 6F 6E 20 63 33 34 ub..Function c34
37 66 66 63 66 28 64 33 62 66 61 62 36 66 29 0D 7ffcf(d3bfab6f).
0A 63 33 34 37 66 66 63 66 20 3D 20 53 74 72 43 .c347ffcf = StrC
6F 6E 76 28 64 33 62 66 61 62 36 66 2C 20 36 34 onv(d3bfab6f, 64
29 0D 0A 45 6E 64 20 46 75 6E 63 74 69 6F 6E 0D )..End Function.
0A 46 75 6E 63 74 69 6F 6E 20 63 64 63 61 31 37 .Function cdca17
```

Recorded Actions:

Action	Parameters	Description
Found Entry Point Open	autoopen ['GET', "ActiveDocument.Shapes('1').AlternativeText", False]	Interesting Function Call
GET	ActiveDocument.Shapes('1').AlternativeText	Interesting Function Call
CreateObject	['Scripting.FileSystemObject']	Interesting Function Call
CreateTextFile	['c:\programdata\preview.jpeg']	Interesting Function Call
Dropped File Hash	21726c10dcf9e11a1bc65ffab39bb4df9a068d87d16f1946d8f54d44860395a5	File Name: c:/programdata/preview.jpeg
CreateObject Execute Command	['wscript.shell'] ActiveDocument.Shapes('1').Title c:\programdata\preview.jpeg	Interesting Function Call Shell function

6. ccSubSDK database

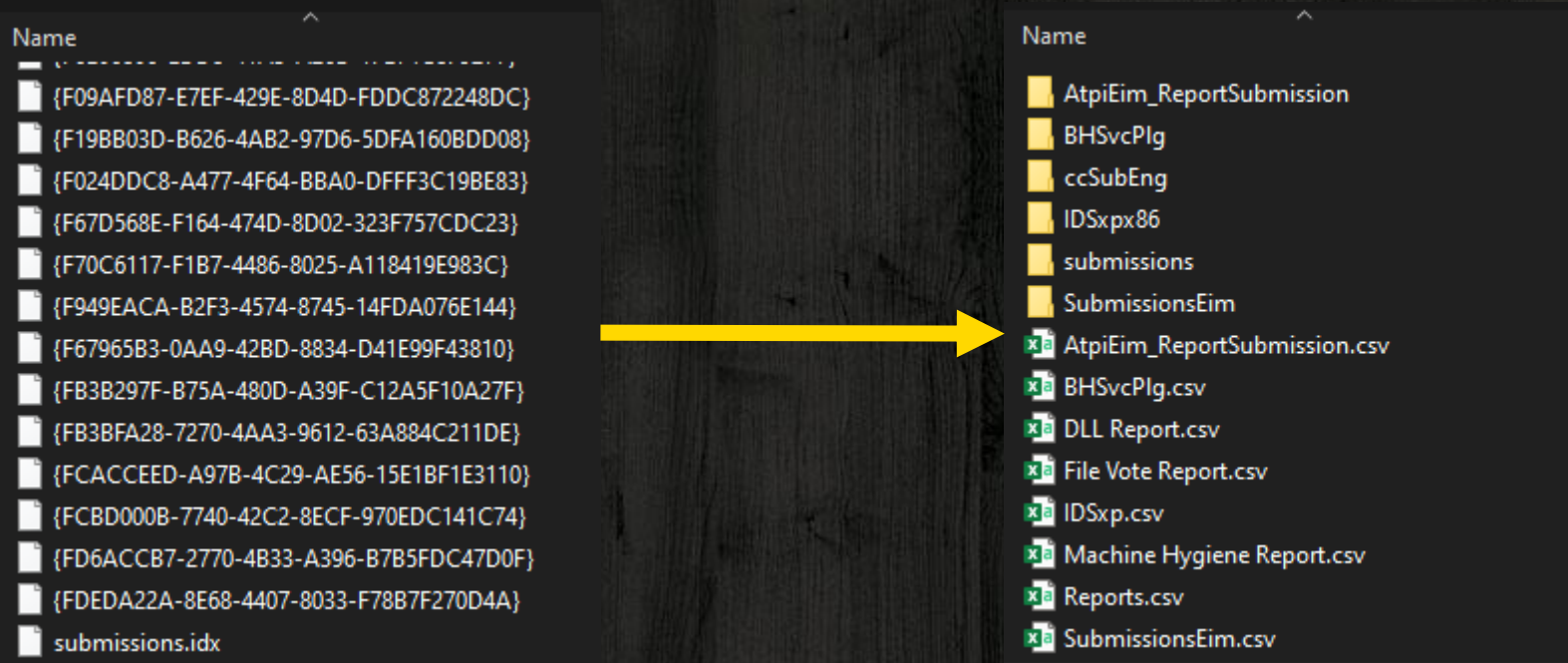
Symantec submission data

ccSubSDK database

- ◆ Submit pseudonymous information about detections, network, and configuration to Symantec Security Response
- ◆ Includes information about antivirus detections, intrusion prevention, SONAR, and file reputation detections

ccSubSDK database

- ◆ Blowfish encrypted database consisting of an index file and GUID files



Final Thoughts

- ◆ By looking at the endpoint logs, VBNs and ccSubSDK we can:
 - Get the hash of the file
 - Creation/Modify/Access/Quarantine times
 - Certificate information
 - SDDL of file
 - And more...
- ◆ This is even before extracting the quarantined data



Thanks!

Any questions?

You can find me at:

Twitter [@bmmaloney97](https://twitter.com/bmmaloney97)

<https://github.com/Beercow/SEPparser>

<https://malwaremaloney.blogspot.com/p/all-things-symantec.html>

