Your AV is Trying to Tell You Something: Submission Engine

malwaremaloney.blogspot.com/2021/03/your-av-is-trying-to-tell-you-something_23.html

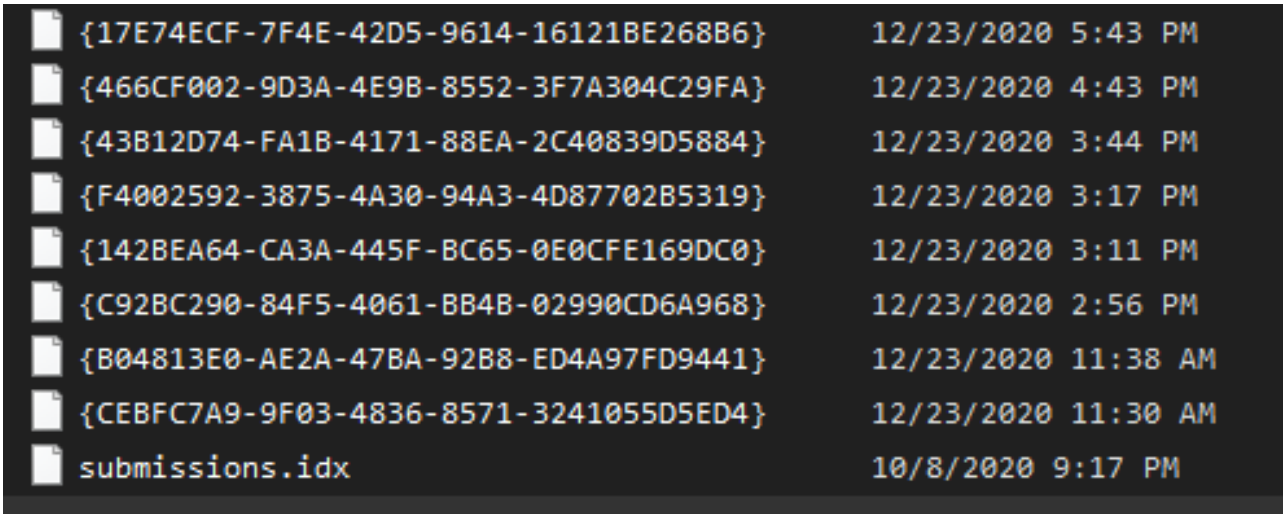
ccSubSDK

"Symantec Endpoint Protection clients automatically submit pseudonymous information about detections, network, and configuration to Symantec Security Response. Symantec uses this pseudonymous information to address new and changing threats as well as to improve product performance. Pseudonymous data is not directly identified with a particular user.

The detection information that clients send includes information about antivirus detections, intrusion prevention, SONAR, and file reputation detections." [1]

These files can be found at the following location: C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\CmnClnt\ccSubSDK

Inside this folder is the submissions.idx file and series of GUID files. Lets look at the submissions.idx file first.

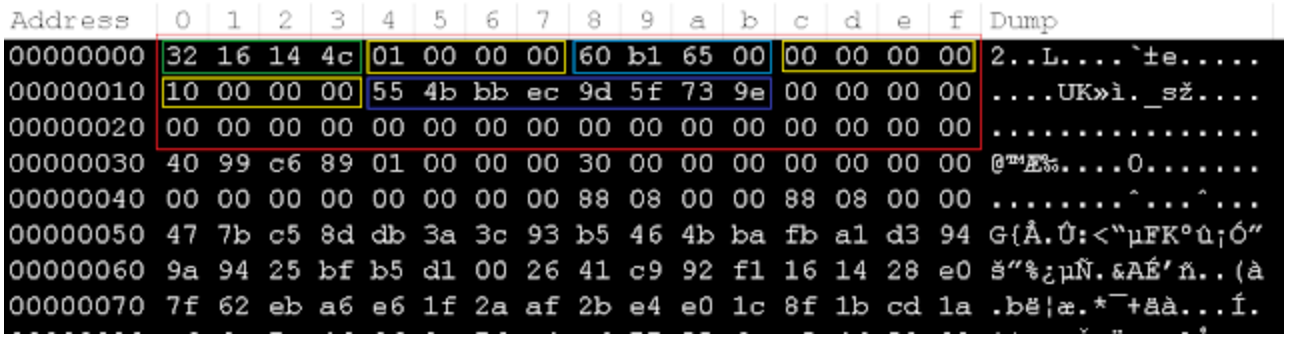


ccSubSDK folder structure

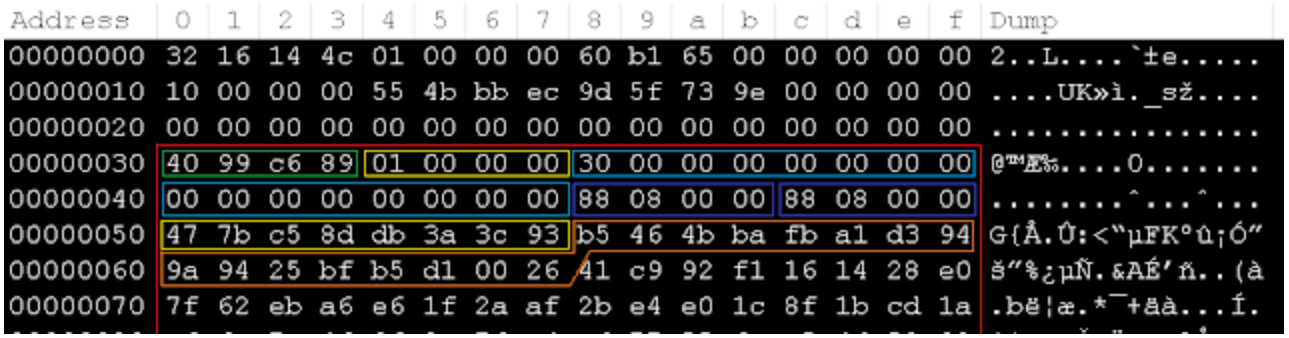
submissions.idx

The submissions.idx file appears to be a type of index for the GUID files. Symantec had a database and word processing software called Q&A form 1985-1998. It just so happens that one of the database extensions was idx. My hypothesis is Symantec is either using their old database format, or parts of it, to index and send submission data back to their servers.

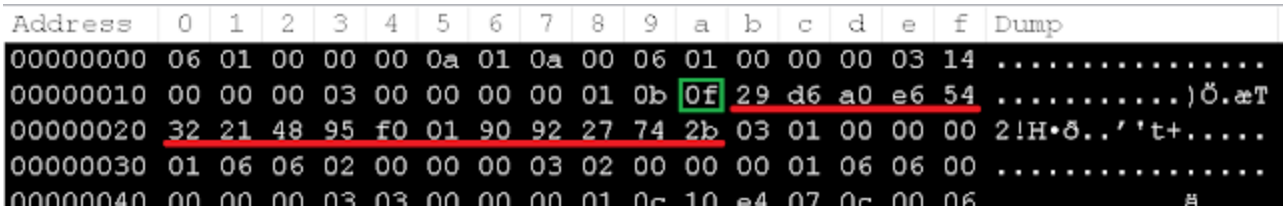
The format of the file is fairly simple. It contains a header and a series of indexed data that points back the GUID files. The header starts with 0x3216144C and contains the size of the submissions.idx file. After the header comes the indexes.



Each index contains a header starting with 0x4099C689. This header contains information on the offset of the current and previous index, the size of the data, and the Blowfish key to decrypt the data. Once the data is decrypted, we can see the information that it contains.



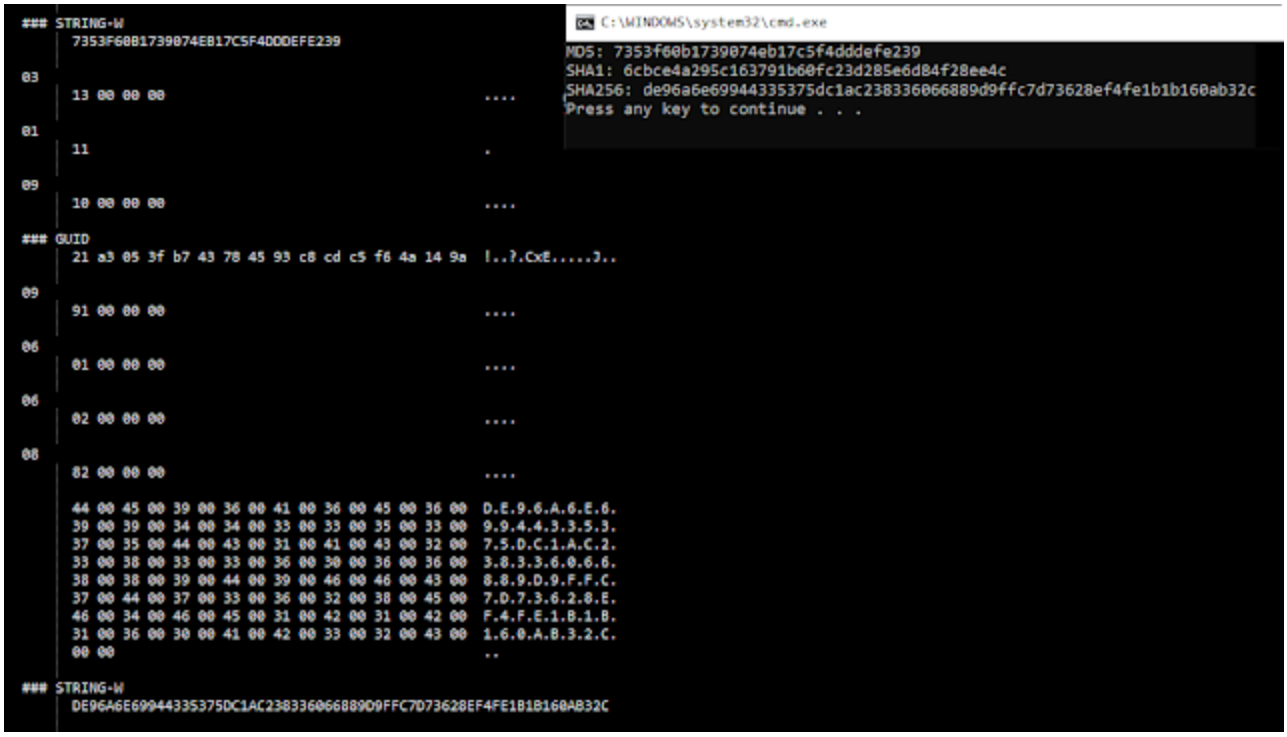
The data is in the same ASN.1 format that the VBN files use. If we start following the tags, the first 0x0F we come to is the name of the GUID file this index references.

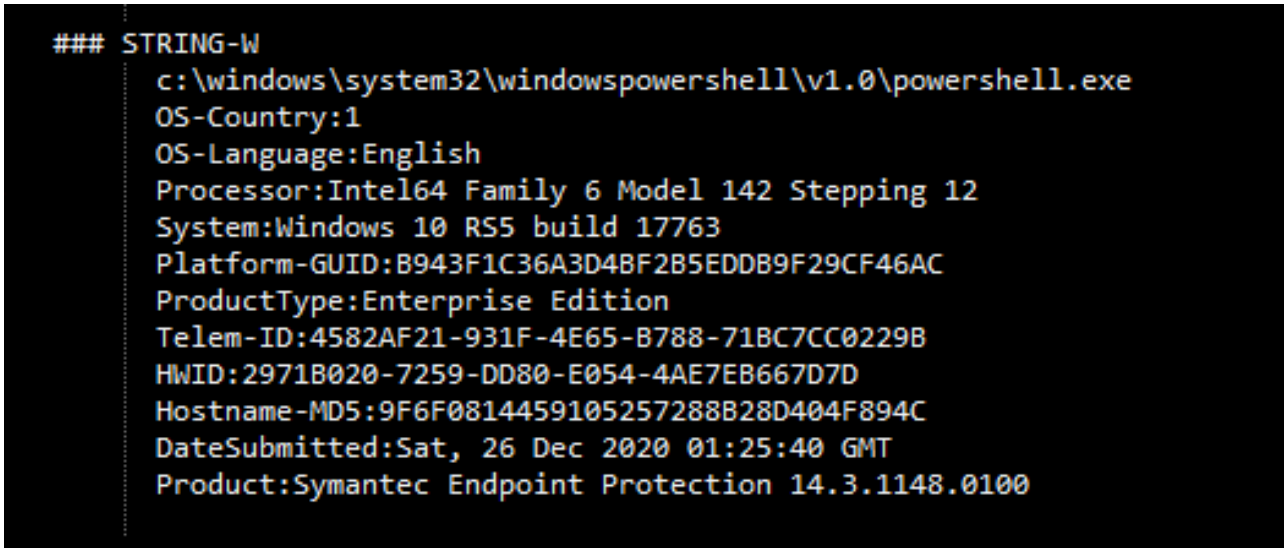


GUID in index

GUID file in ccSubSDK

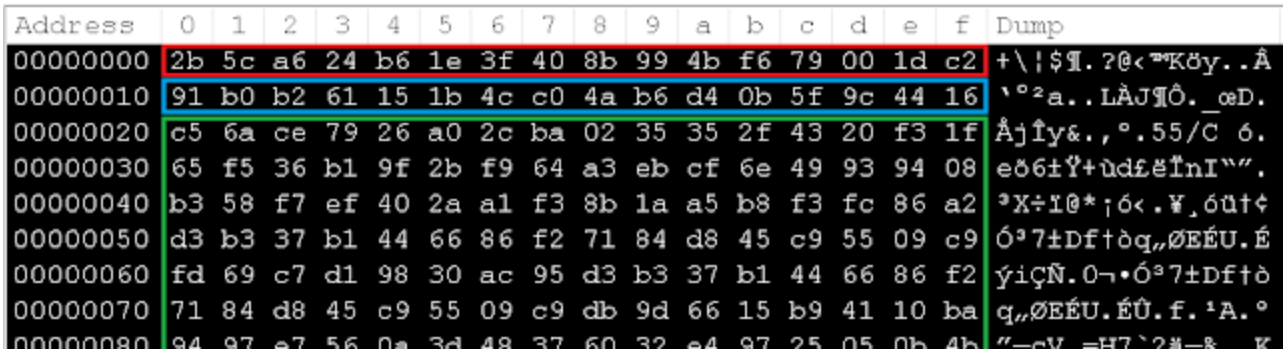
Depending on what type of submission it is, the index will contain information like MD5, SHA256 and some type of report.





{GUID} file

The GUID files hold the information that was submitted to Symantec. The file consists of three parts: the GUID for the dll responsible for the submission, Blowfish key, and the data encrypted with the Blowfish algorithm.



Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	2b	5c	a6	24	b6	1e	3f	40	8b	99	4b	f6	79	00	1d	c2	+\¦$¶.?@‹™Köy..Â
00000010	91	b0	b2	61	15	1b	4c	c0	4a	b6	d4	0b	5f	9c	44	16	‘°²a..LÀJ¶Ô._œD.
00000020	c5	6a	ce	79	26	a0	2c	ba	02	35	35	2f	43	20	f3	1f	Åjîy&.,º.55/C 6.
00000030	65	f5	36	b1	9f	2b	f9	64	a3	eb	cf	6e	49	93	94	08	eõ6±Ÿ+ùd£ëÏnI“”.
00000040	b3	58	f7	ef	40	2a	a1	f3	8b	1a	a5	b8	f3	fc	86	a2	³X÷ï@*¡ó‹.¥¸óü†¢
00000050	d3	b3	37	b1	44	66	86	f2	71	84	d8	45	c9	55	09	c9	Ó³7±Df†òq„ØEÉU.É
00000060	fd	69	c7	d1	98	30	ac	95	d3	b3	37	b1	44	66	86	f2	ýiÇÑ.0¬•Ó³7±Df†ò
00000070	71	84	d8	45	c9	55	09	c9	db	9d	66	15	b9	41	10	ba	q„ØEÉU.ÉÛ.f.¹A.º
00000080	94	97	e7	56	0a	3d	48	37	60	32	e4	87	25	05	0b	4b	“—çV.=H7`2ä‡%..K

The following dll GUID's have been identified.

- 2B5CA624B61E3F408B994BF679001DC2 = BHSvcPlg
- 334FC1F5F2DA574E9BE8A16049417506 = SubmissionsEim
- 38ACED4CA8B2134D83ED4D35F94338BD = SubmissionsEim
- 5E6E81A4A77338449805BB2B7AB12FB4 = AtpiEim, ReportSubmission
- 6AB68FC93C09E744B828A598179EFC83 = IDSxpx86
- 95AAE6FD76558D439889B9D02BE0B850 = IDSxpx86
- 6A007A980A5B0A48BDFC4D887AEACAB0 = IDSxpx86
- D40650BD02FDE745889CB15F0693C770 = IDSxpx86
- 3DC1B6DEBAE889458213D8B252C465FC = IDSxpx86
- 8EF95B94E971E842BAC952B02E79FB74 = AVModule
- A72BBCC1E52A39418B8BB591BDD9AE76 = RepMgtTim
- F2ECB3F7D763AE4DB49322CF763FC270 = ccSubEng

Once the submission has been decrypted, we can look at the data. This can hold anything from the detection information, network data, attack data, detection digest, and even the file itself!

Information was derived from @hexicorn
https://www.hexacorn.com/blog/2016/09/15/dexray-1-6-ccsubsdk-files/
https://www.hexacorn.com/blog/2016/09/18/dexray-1-7-ccsubsdk-files-part-2/

submissions.idx

Header

Offset	Length	Field	Description
0	4	Header	Always 0x3216144C
4	4	Unknown	Will require further investigation as to the purpose of this entry.
8	4	Size	Size of submissions.idx

Offset	Length	Field	Description
12	4	Unknown	Will require further investigation as to the purpose of this entry.
16	4	Unknown	Will require further investigation as to the purpose of this entry.
20	8	Unknown	Will require further investigation as to the purpose of this entry.
28	20	Unknown	Will require further investigation as to the purpose of this entry.

Index

Continues to end of file.

Offset	Length	Field	Description
0	4	Header	Always 0x4099C689
4	4	Unknown	Will require further investigation as to the purpose of this entry.
8	8	Start of Index	Offset to begining of Index
16	8	Start of Last Index	Offset to begining of previous Index
24	4	Lenght 1	Total size of Data including Blowfish Key
28	4	Lenght 2	Actual size of Data including Blowfish Key ***If length is 0, record is deleted.**
32	8	Unknown	Will require further investigation as to the purpose of this entry.
40	16	Blowfish Key	Symmetric-key for Blowfish

Offset	Length	Field	Description
56	Length 1 - 16	Data	Data appears to be in ASN.1 format. It is comprised of a series of tags.

Code	Value Length	Extra Data
0x01	1	None
0x0A	1	None
0x03	4	None
0x06	4	None
0x04	8	None
0x07	4	NUL-terminated ASCII String (of length controlled by dword following 0x07 code)
0x08	4	NUL-terminated Unicode String (of length controlled by dword following 0x08 code)
0x09	4	Container (of length controlled by dword following 0x09 code)
0x0F	16	None
0x10	16	None

{GUID} Files

{GUID} files can be found in the following location: C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\CmnClnt\ccSubSDK\{GUID}

Offset	Length	Field	Description
0	16	GUID	GUID of dll responsible for submission.
16	16	Blowfish Key	Symmetric-key for Blowfish

Offset	Length	Field	Description
32	varies	Data	Data appears to be in ASN.1 format. It is comprised of a series of tags.

Code	Value Length	Extra Data
0x01	1	None
0x0A	1	None
0x03	4	None
0x06	4	None
0x04	8	None
0x07	4	NUL-terminated ASCII String (of length controlled by dword following 0x07 code)
0x08	4	NUL-terminated Unicode String (of length controlled by dword following 0x08 code)
0x09	4	Container (of length controlled by dword following 0x09 code)
0x0F	16	None
0x10	16	None