Caution! Ryuk Ransomware decryptor damages larger files, even if you pay

blog.emsisoft.com/en/35023/bug-in-latest-ryuk-decryptor-may-cause-data-loss/

December 9, 2019

Ransomware

- Emsisoft Malware Lab
- December 9, 2019
- 3 min read

Ryuk has plagued the public and private sectors alike over the past years, generating hundreds of millions of ransom revenues for the criminals behind it. Usually deployed via an existing malware infection within a target's network, Ryuk wreaks havoc on any system that can be accessed, encrypting data using a combination of RSA and AES.

Just because Ryuk has been hugely successful, doesn't mean its creators stopped evolving and improving it, however. So it comes to no surprise that we have seen multiple new features added to Ryuk over the past year.

One of these features that isn't well documented is its capability to partially encrypt files. Essentially, whenever Ryuk encounters a file that is larger than 57,000,000 bytes (or 54.4 megabytes) it will only encrypt certain parts of it in order to save time and allow it to work its way through the data as quickly as possible before anyone notices.

```
BlocksToEncrypt = 0i64;
if ( FileSize_1.QuadPart > 57000000ui64 )
{
  BlocksToEncrypt = 27 * FileSize_1.QuadPart / 100ui64 / 1000000;
  if ( FileSize_1.QuadPart <= 10000000000ui64 )
  {
    if ( FileSize_1.QuadPart <= 1000000000ui64 || FileSize_1.QuadPart >= 10000000000ui64 )
    {
      if ( FileSize_1.QuadPart < 1000000000ui64 )
        BlocksToEncrypt = 27 * FileSize_1.QuadPart / 100ui64 / 1000000;
    }
    else
    {
      BlocksToEncrypt = 15 * FileSize_1.QuadPart / 100ui64 / 1000000;
    }
  }
  else
  {
    BlocksToEncrypt = 7 * FileSize_1.QuadPart / 100ui64 / 1000000;
    if ( BlocksToEncrypt > 0xFA0 )
      BlocksToEncrypt = 2000i64;
  }
}
if ( BlocksToEncrypt > 2000 || !(_DWORD)BlocksToEncrypt )
  BlocksToEncrypt = 2000i64;
v26 = FileSize_1;
if ( FileSize_1.QuadPart < 25ui64 )
{
  dword_3016E018(hFile);
  return 2;
}
```

The code used by Ryuk to determine how much of a file to encrypt if the file exceeds a size limit of 57,000,000 bytes

Files that are only partially encrypted will show a slightly different-than-normal footer at the end of the file, where Hermes usually stores the RSA-encrypted AES key that was used to encrypt the file's content. In addition to the HERMES files marker used by Ryuk, you will also find a clearly visible counter of how many 1,000,000 bytes blocks have been encrypted for this file. If that indicator is missing, the whole file is considered to be encrypted.

7C	32	31	7C	48	45	52	4D	45	53	01	02	00	00	10	66	|21|HERMES.....f
00	00	00	A4	00	00	A2	22	AF	76	B7	06	7A	98	5E	6D	...¤..¢"¯v·.z˜^m
5A	64	E1	DF	A3	F8	58	CE	FF	24	1A	D9	71	66	BE	69	Zdáß£øXÎÿ$.Ùqf¾i
95	DE	6B	EE	D6	24	80	9C	E4	8F	CC	32	C6	85	5A	FA	•ÞkîÖ$€œä.Ì2Æ…Zú
A2	38	BC	2F	DC	8F	F8	A4	DB	F7	26	84	FF	92	7B	81	¢8¼/Ü.ø¤Û÷&„ÿ'{.
E5	12	B5	B4	53	50	2D	52	6A	94	05	FB	3B	F4	0E	02	å.µ´SP-Rj".û;ô..
91	79	1E	5C	C8	D4	BB	09	0D	F5	1F	7D	FD	8D	67	75	'y.\ÈÔ»..õ.}ý.gu
74	FF	C4	E4	77	9A	E8	59	32	22	27	1C	73	88	BD	EE	tÿÄäwšèY2"'.s^½î
B2	A2	26	FF	C2	D5	74	24	E0	BA	57	A4	2F	94	61	B6	²¢&ÿÂÕt$à°W¤/"a¶
50	33	EC	A1	40	CA	AE	DB	E9	1C	E0	85	3C	80	0E	C4	P3ì¡@Ê®Ûé.à…<€.Ä
11	2D	95	B7	4E	A6	38	60	D6	F2	3D	CF	66	45	DA	42	.-•·N¦8`Öò=ÏfEÚB
2F	67	F0	45	67	B2	BD	87	68	85	0F	AF	3E	19	9E	B8	/gðEg²½‡h….¯>.ž¸
8B	BB	47	AC	D1	5D	0C	86	2A	81	CB	D2	1F	8D	AE	1F	‹»G¬Ñ].†*.ËÒ..®.
FA	46	00	37	50	D3	33	1F	D9	C9	1A	38	40	F1	20	91	úF.7PÓ3.ÙÉ.8@ñ '
1C	5F	82	3B	16	50	1B	18	29	4A	37	20	A4	6E	1F	B7	._‚;.P..)J7 ¤n.·
A2	50	00	4C	04	C1	CE	0B	4B	C9	85	81	3D	CF	F2	E0	¢P.L.ÁÎ.KÉ….=Ïòà
47	B8	66	8A	99	DD	43	64	ED	68	A7	0A	79	EA	57	D6	G¸fŠ™ÝCdíh§.yêWÖ
11	31	F4	13	39	69	00	00	00	00	00	00	00	00	00	00	.1ô.9i..........
00	00	00	00	00	00											......

The extended version of the Ryuk file footer highlighting the number of encrypted blocks for partially encrypted files

In one of the latest versions of Ryuk, changes were made to the way the length of the footer is calculated. As a result, the decryptor provided by the Ryuk authors will truncate files, cutting off one too many bytes in the process of decrypting the file. Depending on the exact file type, this may or may not cause major issues. In the best-case scenario, the byte that was cut off by the buggy decryptor was unused and just some slack space at the end created by aligning the file towards certain file size boundaries. However, a lot of virtual disk type files like VHD/VHDX as well as a lot of database files like Oracle database files will store important information in that last byte and files damaged this way will fail to load properly after they are decrypted.

One of the services we provide at Emsisoft is to help ransomware victims who paid the ransom to recover their files even if the ransomware authors left them hanging by either being uncooperative or providing tools that do not do the job properly, both of which are increasingly common outcomes.

So if you are a Ryuk victim that was hit within the last two weeks and have files which will not load, please contact us so we can provide you with a properly working decryptor. Please understand that this will only work if you still have copies or backups of your encrypted data, as the Ryuk decryptor will usually delete files it thinks were decrypted properly. Similarly, if you've paid for a decryptor but have yet to use it, either back up your files before running it or get in touch with us instead. Our tool will enable you to safely recover your data whereas the tool supplied by the bad actors will not.

Note our decryption tool does not remove the need for ransoms to be paid; it is simply a replacement for the criminal-supplied tool.

A final word of advice: prior to running any ransomware decryptor – whether it was supplied by a bad actor or by a security company – be sure to back up the encrypted data first. Should the tool not work as expected, you'll be able to try again.

Emsisoft Malware Lab

The Lab team is a group of cybersecurity researchers whose mission is to enhance protection in Emsisoft products, help organizations respond to security incidents and create analysis that helps decision-makers understand the threat landscape.