A Technical Analysis of Royal Ransomware

Prepared by: Vlad Pasca, Senior Malware & Threat Analyst

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com

Tower 49
12 E 49th Street
Suite 15-001
New York, NY 10017
1.800.682.1707

Table of contents

Executive summary

Royal ransomware is a recent threat that appeared in 2022 and was particularly active during recent months. The ransomware deletes all Volume Shadow Copies and avoids specific file extensions and folders. It encrypts the network shares found in the local network as well as the local drives. A parameter called “-id” that identifies the victim and is also written in the ransom note must be specified in the command line.

The files are encrypted using the AES algorithm (OpenSSL), with the key and IV being encrypted using the RSA public key that is hard-coded in the executable. The malware can fully or partially encrypt a file based on the file’s size and the “-ep” parameter. The extension of the encrypted files is changed to “.royal”.

Analysis and findings

SHA256: f484f919ba6e36ff33e4fb391b8859a94d89c172a465964f99d6113b55ced429

The malware is a 64-bit executable that is not packed. It retrieves the command-line string for the process using the GetCommandLineW API:

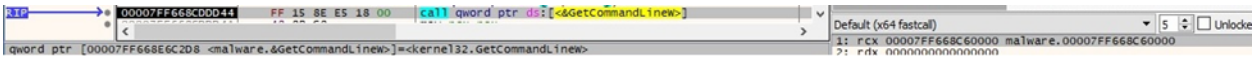


Figure 1

CommandLineToArgvW is utilized to obtain an array of pointers to the command line arguments, as highlighted below:

Figure 2

The process compares the arguments with "-path", "-id", and "-ep". The “-id” parameter is mandatory and consists of 32 characters that could be a victim ID. In this case, any 32 characters value can be specified (see figure 3).

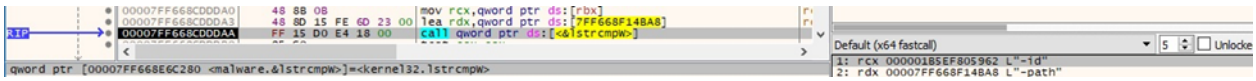


Figure 3

The ransomware deletes all Volume Shadow Copies by spawning a vssadmin.exe process:

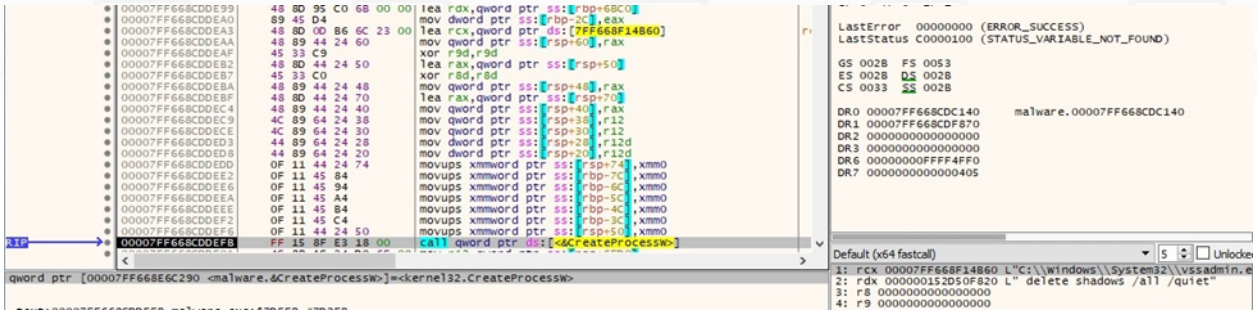


Figure 4

The malware decrypts a list of extensions that will be skipped:

- .exe
- .dll
- .bat
- .lnk
- .royal

A list of directories to be skipped is also decrypted:

- windows
- royal
- $recycle.bin
- google
- perflogs
- mozilla
- tor browser
- boot
- $windows.~ws
- $windows.~bt
- windows.old

The executable initiates the use of the Winsock DLL via a function call to WSAStartup:

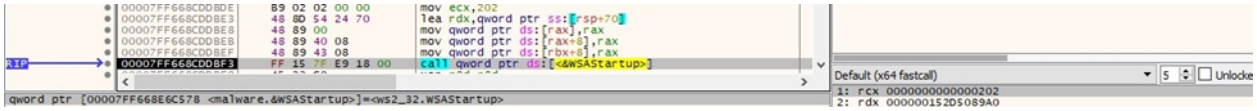


Figure 5

A new socket is created using the socket API (0x2 = **AF_INET**, 0x1 = **SOCK_STREAM**):

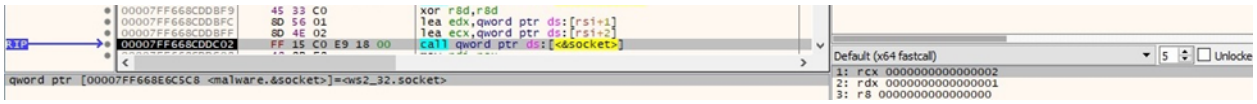


Figure 6

The binary obtains a pointer to an extension function using the WSAIoctl routine (0xC8000006 = **SIO_GET_EXTENSION_FUNCTION_POINTER**):

Figure 7

The GetNativeSystemInfo API is used to extract information about the current system:

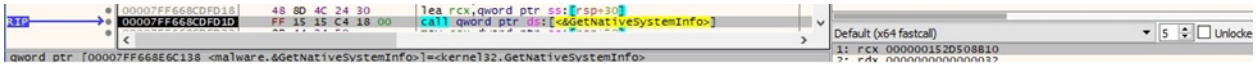


Figure 8

The malicious process creates multiple threads depending on the number of available processors responsible for files' encryption:

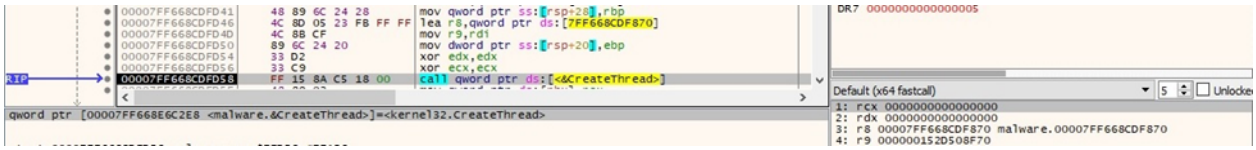


Figure 9

A single thread that executes the StartAddress function takes care of the files' enumeration:

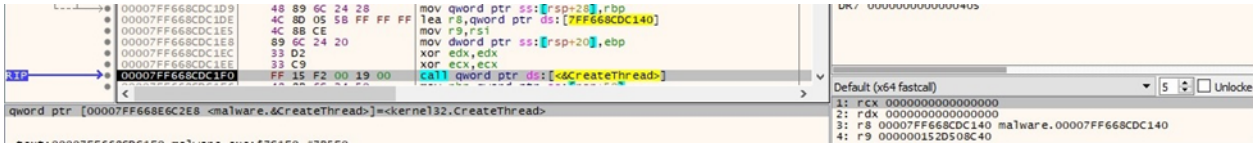


Figure 10

The GetIpAddrTable function retrieves the interface-to-IPv4 address mapping table (see figure 11).

Figure 11

The IP addresses extracted from the above table are converted from network order to host byte order, as displayed in figure 12.

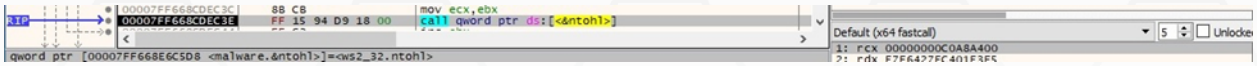


Figure 12

Royal ransomware creates an input/output (I/O) completion port that is not yet associated with a file handle using CreateIoCompletionPort:

Figure 13

The WSASocketW routine is used to create a socket that is bound to the TCP protocol (0x2 = **AF_INET**, 0x1 = **SOCK_STREAM**, 0x6 = **IPPROTO_TCP**):

Figure 14

The process associates the local address with the above socket, as shown in figure 15.

Figure 15

The I/O completion port that was already created is associated with the TCP socket via a function call to CreateIoCompletionPort:

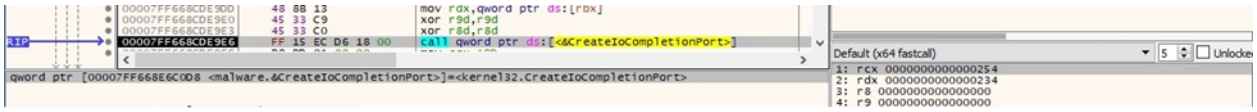


Figure 16

The malware tries to iteratively connect to other hosts in the same network on port 445:

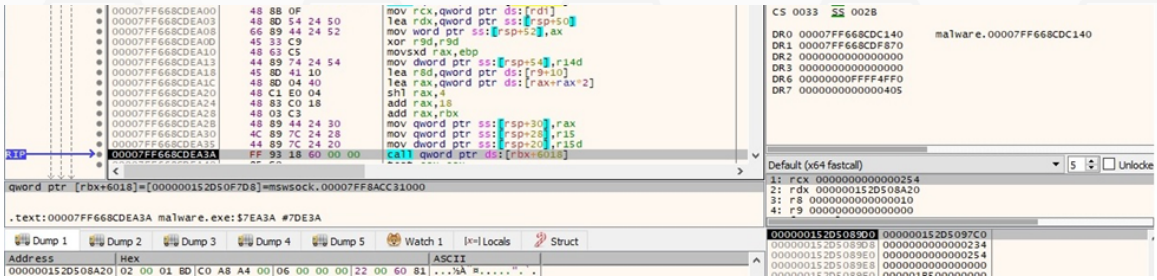


Figure 17

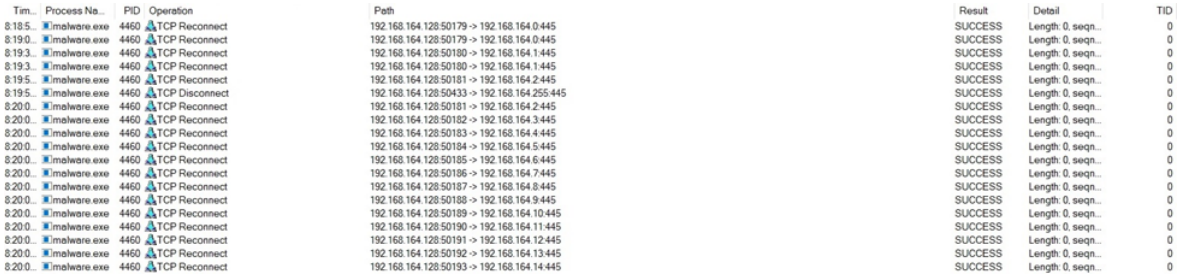


Figure 18

The malicious executable dequeues an I/O completion packet from the I/O completion port by calling the GetQueuedCompletionStatus API:

Figure 19

The WSAAddressToStringW routine is utilized to extract the reachable IP addresses from the sockaddr structures:

Figure 20

The ransomware enumerates the network shares that are different than "ADMIN$" and "IPC$":

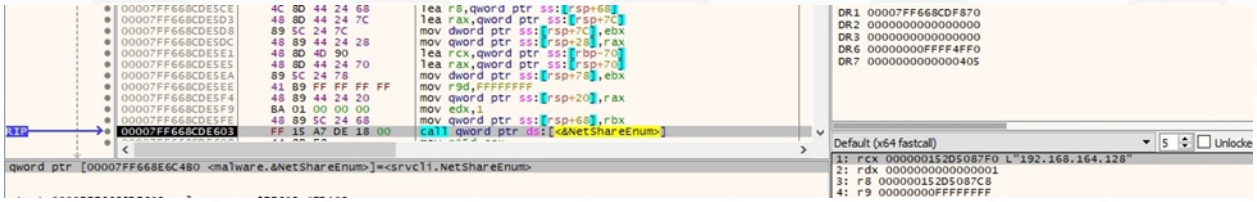


Figure 21

Thread activity – StartAddress function

GetLogicalDrives is used to obtain the currently available disk drives (see figure 22).

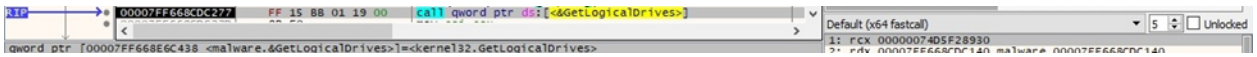


Figure 22

A ransom note called “README.txt” is created in every drive (0x40000000 = **GENERIC_WRITE**):

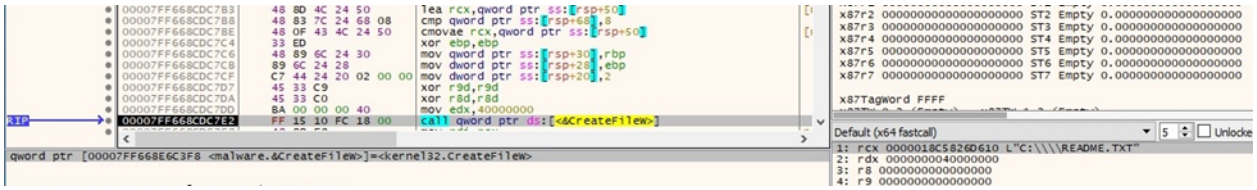


Figure 23

The ransom note containing the “-id” parameter is populated using the WriteFile routine:

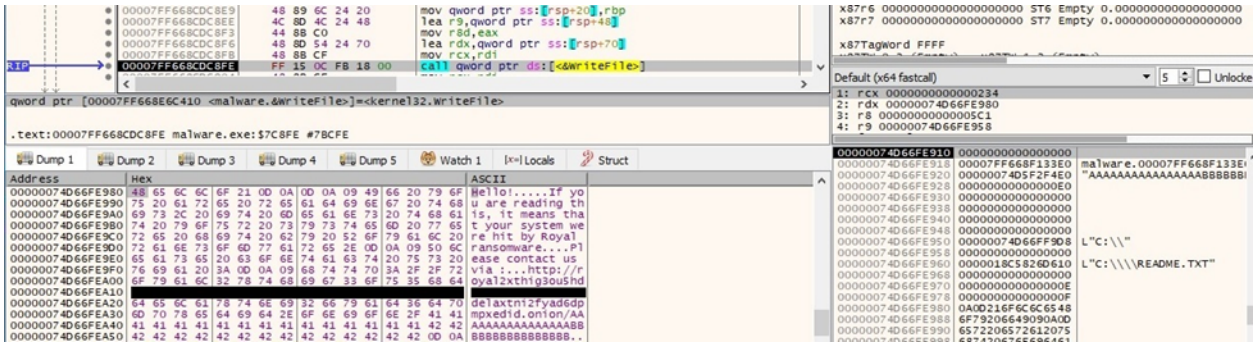


Figure 24

The ransomware starts enumerating the files using the FindFirstFileW function:

Figure 25

It compares the directories name with the list of excluded folders using StrStrIW:

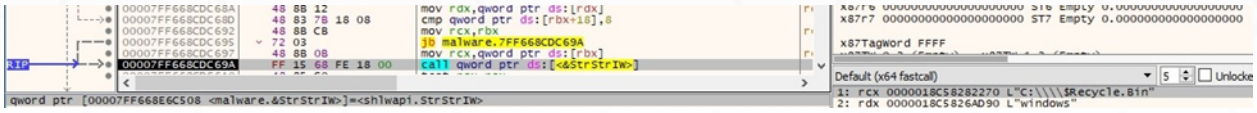


Figure 26

The files enumeration continues by calling the FindNextFileW API:

Figure 27

Thread activity – sub_7FF668CDF870 function

The malware imports a hard-coded RSA public key:

```
String          db '-----BEGIN RSA PUBLIC KEY-----',0Ah
                                        ; DATA XREF: sub_7FF668CDF870+49↑o
                                        ; sub_7FF668CDF870+59↑o ...
                db 'MIICCAKCAgEAuWfX+pJCUCKc9xsWLVHpCpw6TL20HG/Vk4vF3GYlr6HltX7BMRfA',0Ah
                db '7oGyMztNb37xW66NX+uxHghrX3+sm23yJmSfressJIGOvDNZVO80JevZxuhHUome',0Ah
                db 'RdLfjRYpuEg8mbEdL1c1jQqoEZEhOIb8Lhv1dBDnwXEBGnf/k8uMuY784xxDfbpt',0Ah
                db 'SB15OOHRfvIqMcIbskQ8RfMDFeiwYNRVrCkyhXOTB+RkmzTtp7q8gjnA1AHOfHSx',0Ah
                db 'eOBVt9Lz27uuS4RIf/b31aiBolzAWft44wSC4diYvSom93d6S2K6oMYNOQvSu+zI',0Ah
                db 'U8/yzxebDN0bWJLVPZxndQFBVHiTXQfWDi1BdsaljR2BHPj/tYWd4j/72vN1vywt',0Ah
                db 'M3sn5TJNql/gJZ7HuU0QOyBzdLk3vpmmqby5wwXLd+WKPWv3HEKaOy80K0F7FrhC',0Ah
                db '0g3nbKAf5Y+MzkEUNHDvwTk9uKY6IlCJ0/fXE78ULcxrgy0w76WVZWweLrsVun5k',0Ah
                db 'J9i+LhcBNH7DJGJ544zC1yFi7sBgeW00VYCh7Ur4o0aE2EwTNYeLIgsFf4A6mOE0',0Ah
                db '6gfoRDNH40U4DdK5JFQRp2tLXI93o7hSEEWAhJe7s0LyD1DLXksQjNkRUe+Ojd5G',0Ah
                db 'AGdM3G7RZuWrMC4FfmtPlzYfdl5o2k/u9RYi7fi8pU34GQvvPhW8wK8CAQM=',0Ah
                db '-----END RSA PUBLIC KEY-----',0Ah
```

Figure 28

The OpenSSL library will be used to encrypt the files using the AES algorithm, with the AES key being encrypted using the RSA public key:

```
aRsaSetupBlindi db 'RSA_setup_blinding',0
                                        ; DATA XREF: sub_7FF668CDFE50+60↑o
                                        ; sub_7FF668CDFE50+189↑o ...
                align 8
aCryptoRsaRsaCr db 'crypto\rsa\rsa_crpt.c',0
                                        ; DATA XREF: sub_7FF668CDFE50+6C↑o
                                        ; sub_7FF668CDFE50+195↑o ...
                align 10h
aCryptoBioBioLi db 'crypto\bio\bio_lib.c',0
                                        ; DATA XREF: sub_7FF668CE0150+13D↑o
                                        ; sub_7FF668CE02F0+139↑o ...
                align 8
aBioNewEx       db 'BIO_new_ex',0       ; DATA XREF: sub_7FF668CE0C70+36↑o
                                        ; sub_7FF668CE0C70+B2↑o ...
                align 8
aBioReadIntern  db 'bio_read_intern',0  ; DATA XREF: sub_7FF668CE13F0+2C↑o
                                        ; sub_7FF668CE13F0+FD↑o ...
aBioWriteIntern db 'bio_write_intern',0 ; DATA XREF: sub_7FF668CE1600+CE↑o
                                        ; sub_7FF668CE1600+1DD↑o
                align 20h
aBioPuts        db 'BIO_puts',0         ; DATA XREF: sub_7FF668CE0990+168↑o
                                        ; sub_7FF668CE0990+203↑o ...
                align 10h
aBioGets        db 'BIO_gets',0         ; DATA XREF: sub_7FF668CE06F0+32↑o
                                        ; sub_7FF668CE06F0+8D↑o ...
                align 4
asc_7FF668E6C7DC db ' ',0               ; DATA XREF: sub_7FF668CE0990+84↑o
                                        ; sub_7FF668CE0990+B4↑o ...
                align 20h
aBioCtrl        db 'BIO_ctrl',0         ; DATA XREF: sub_7FF668CE02F0+12D↑o
                align 10h
aBioCallbackCtr db 'BIO_callback_ctrl',0
```

Figure 29

How the ransomware encrypts a file. The CreateFileW API is used to open a targeted file (0x10000000 = **GENERIC_ALL**):

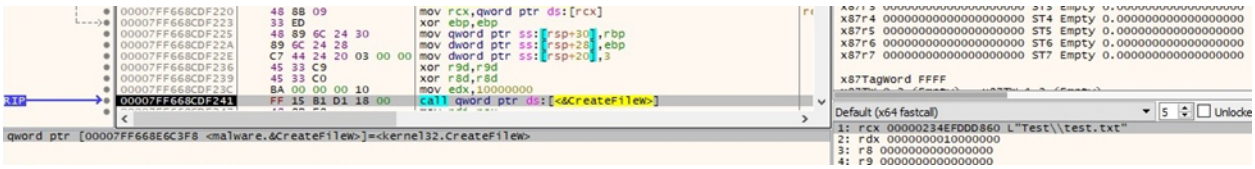


Figure 30

The malicious binary retrieves the size of the file using GetFileSizeEx:

Figure 31

It moves the file pointer to the beginning of the file by calling the SetFilePointerEx routine (0x0 = **FILE_BEGIN**):

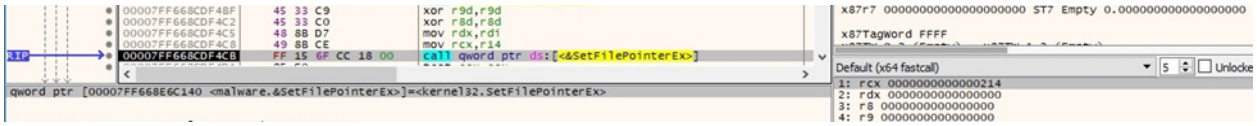
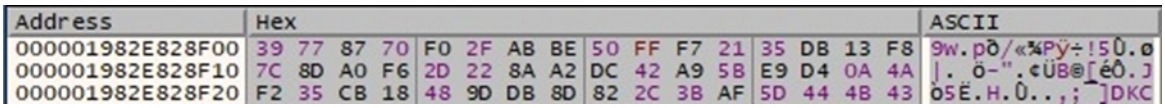


Figure 32

The process generates a random 32-byte AES key and a 16-byte IV using the BCryptGenRandom function (0x2 = **BCRYPT_USE_SYSTEM_PREFERRED_RNG**):

Figure 33



Address	Hex	ASCII
000001982E828F00	39 77 87 70 F0 2F AB BE 50 FF F7 21 35 DB 13 F8	9w.pð/«¾Pÿ÷!5Û.ø
000001982E828F10	7C 8D A0 F6 2D 22 8A A2 DC 42 A9 5B E9 D4 0A 4A	|. ö-".¢ÜB©[éÔ.J
000001982E828F20	F2 35 CB 18 48 9D DB 8D 82 2C 3B AF 5D 44 4B 43	ò5Ë.H.Û..,;¯]DKC

Figure 34

Firstly, the file content is read via a call to ReadFile:

Figure 35

The content is encrypted using the AES256 algorithm 16 bytes at a time (see figure 36). The algorithm implementation can be found here (figure 37).

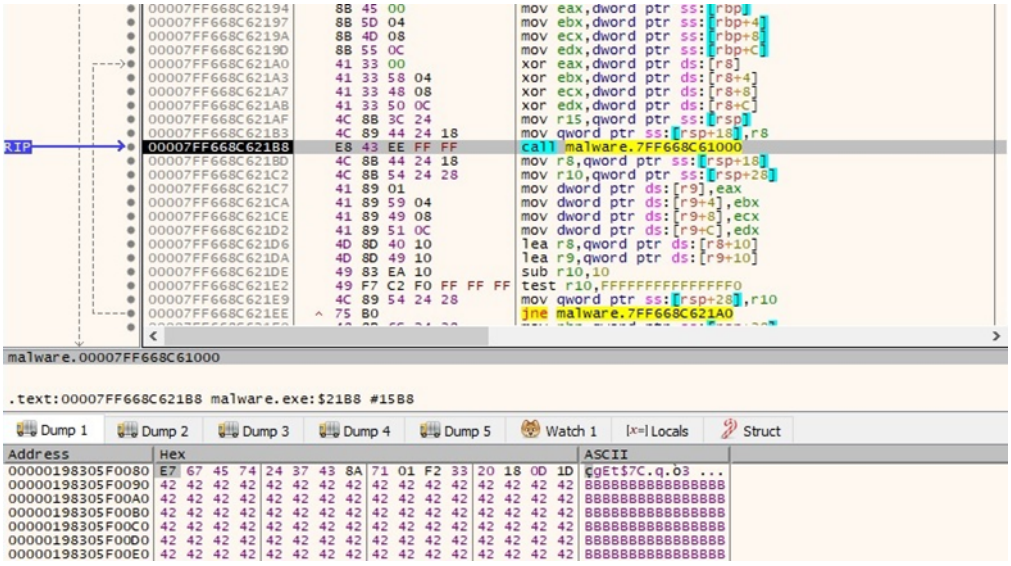


Figure 36

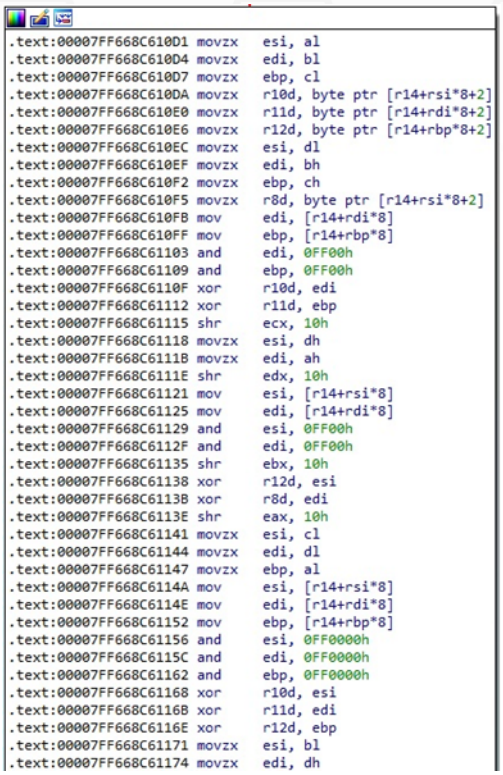


Figure 37

The encrypted content is written back to the file, followed by the AES key and IV that were encrypted using the RSA public key:

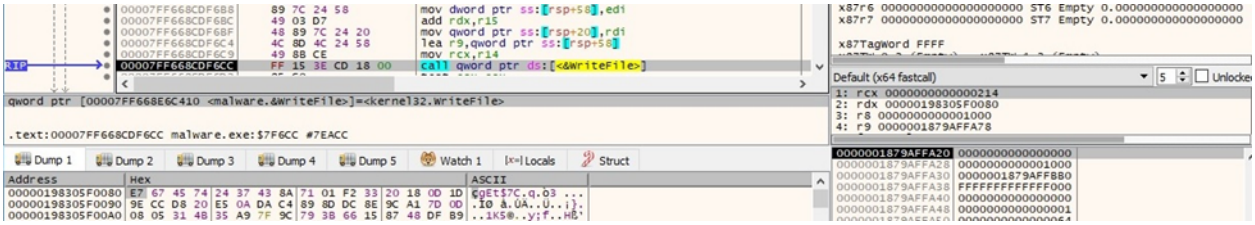


Figure 38

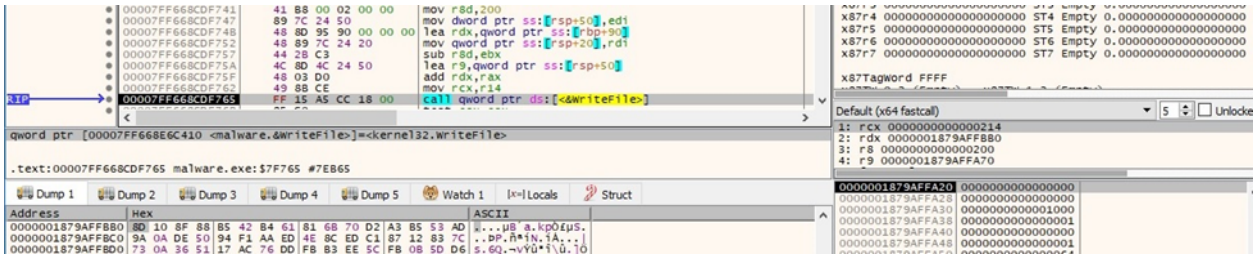


Figure 39

Finally, the ransomware writes the file length and a value representing the encryption

percentage to the file (0x64 = 100%, i.e. the entire file was encrypted):

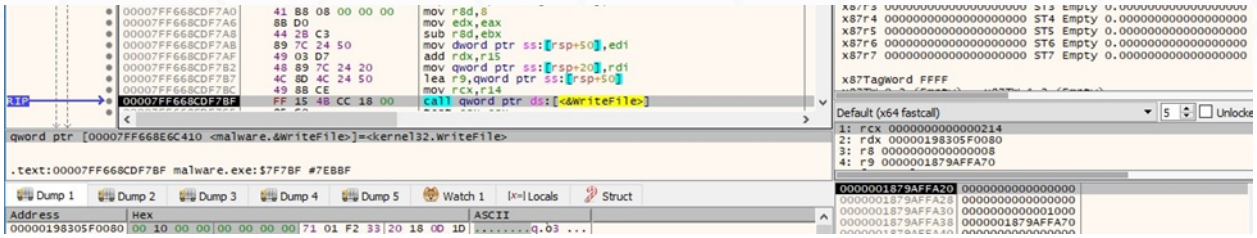


Figure 40

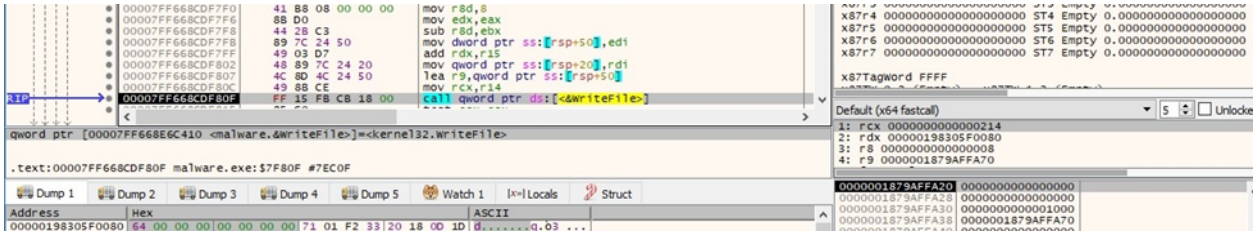


Figure 41

The file's extension is changed to ".royal" using MoveFileExW (0x8 = **MOVEFILE_WRITE_THROUGH**):

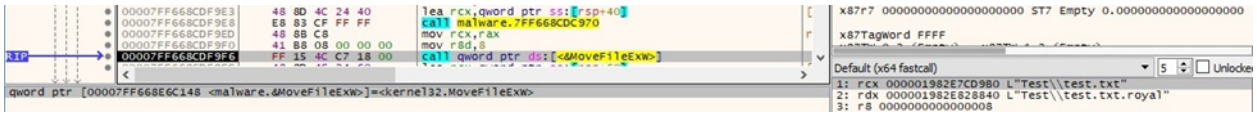
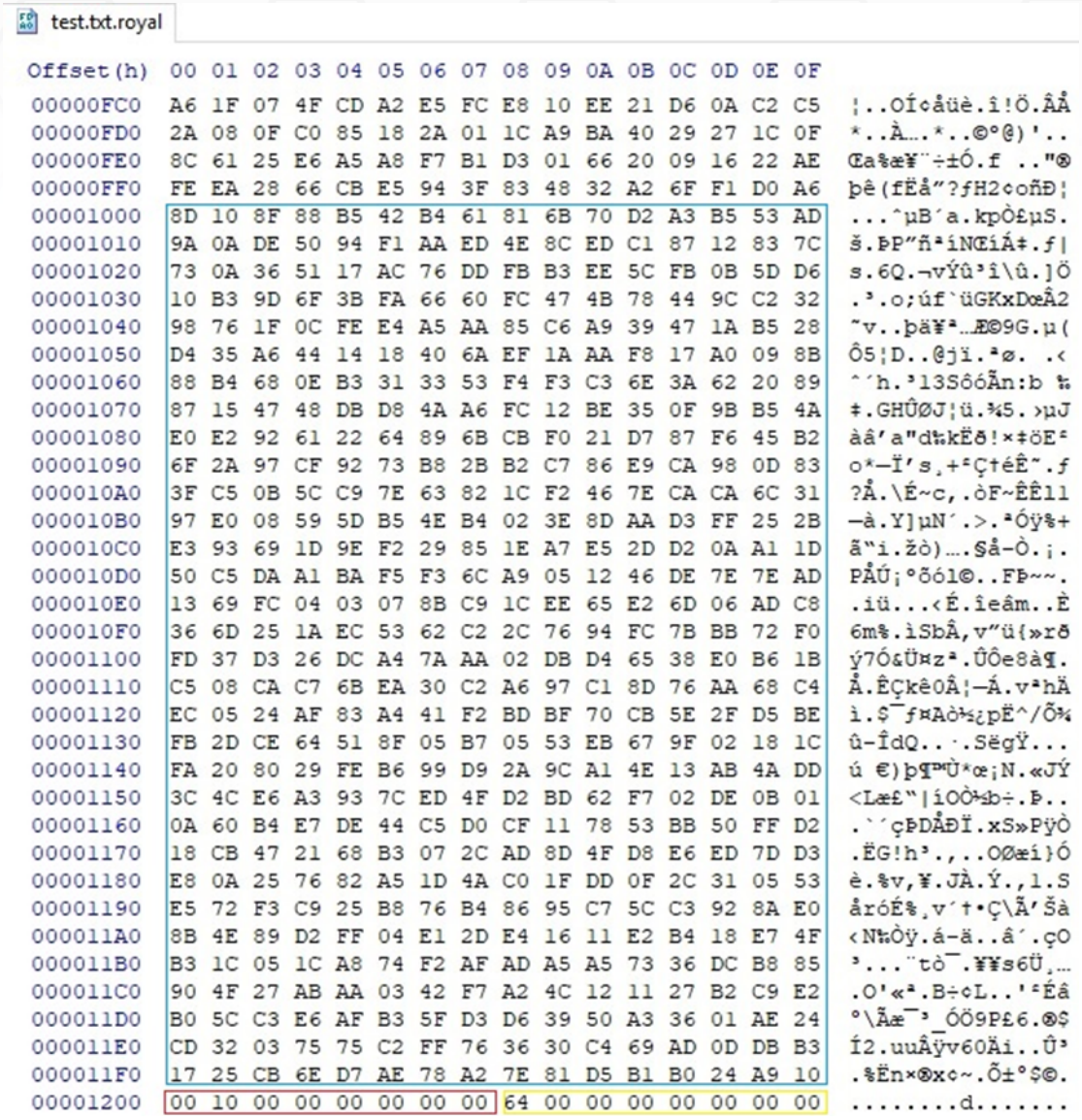


Figure 42

Case 1 – File size < 5244992 bytes (approximately 5MB)

In this case, the entire file is encrypted by the ransomware:



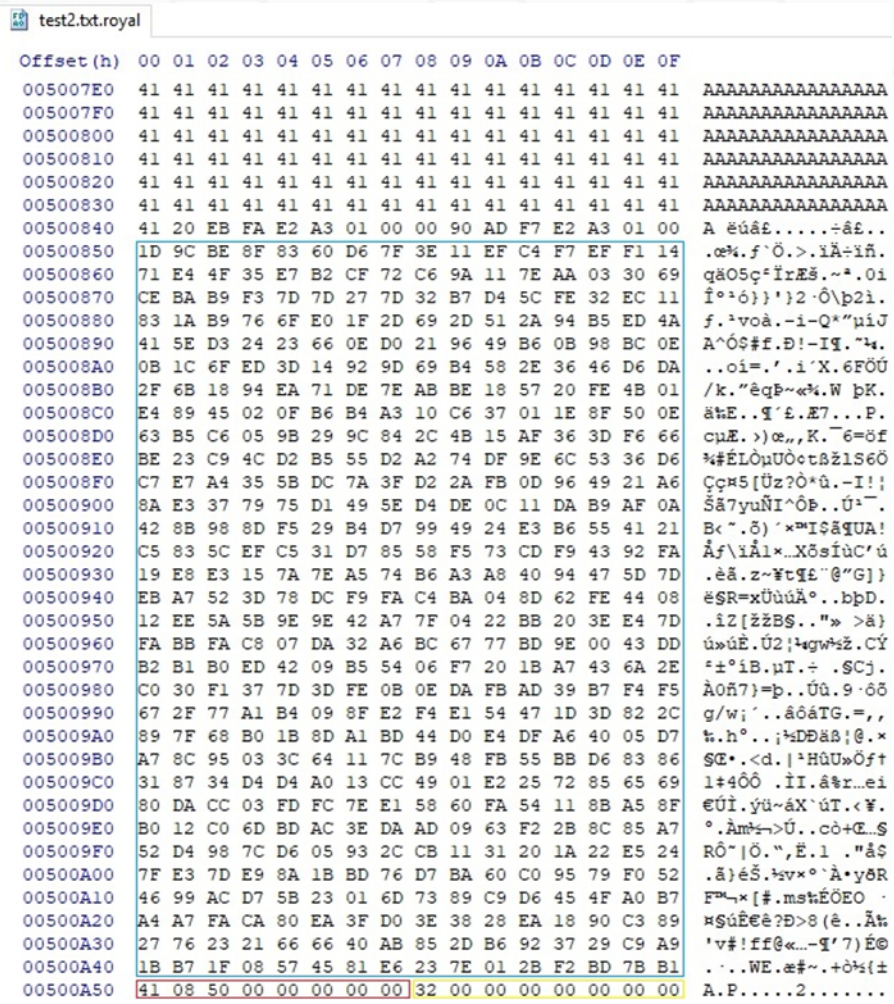
test.txt.royal

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000FC0	A6	1F	07	4F	CD	A2	E5	FC	E8	10	EE	21	D6	0A	C2	C5
00000FD0	2A	08	0F	C0	85	18	2A	01	1C	A9	BA	40	29	27	1C	0F
00000FE0	8C	61	25	E6	A5	A8	F7	B1	D3	01	66	20	09	16	22	AE
00000FF0	FE	EA	28	66	CB	E5	94	3F	83	48	32	A2	6F	F1	D0	A6
00001000	8D	10	8F	88	B5	42	B4	61	81	6B	70	D2	A3	B5	53	AD
00001010	9A	0A	DE	50	94	F1	AA	ED	4E	8C	ED	C1	87	12	83	7C
00001020	73	0A	36	51	17	AC	76	DD	FB	B3	EE	5C	FB	0B	5D	D6
00001030	10	B3	9D	6F	3B	FA	66	60	FC	47	4B	78	44	9C	C2	32
00001040	98	76	1F	0C	FE	E4	A5	AA	85	C6	A9	39	47	1A	B5	28
00001050	D4	35	A6	44	14	18	40	6A	EF	1A	AA	F8	17	A0	09	8B
00001060	88	B4	68	0E	B3	31	33	53	F4	F3	C3	6E	3A	62	20	89
00001070	87	15	47	48	DB	D8	4A	A6	FC	12	BE	35	0F	9B	B5	4A
00001080	E0	E2	92	61	22	64	89	6B	CB	F0	21	D7	87	F6	45	B2
00001090	6F	2A	97	CF	92	73	B8	2B	B2	C7	86	E9	CA	98	0D	83
000010A0	3F	C5	0B	5C	C9	7E	63	82	1C	F2	46	7E	CA	CA	6C	31
000010B0	97	E0	08	59	5D	B5	4E	B4	02	3E	8D	AA	D3	FF	25	2B
000010C0	E3	93	69	1D	9E	F2	29	85	1E	A7	E5	2D	D2	0A	A1	1D
000010D0	50	C5	DA	A1	BA	F5	F3	6C	A9	05	12	46	DE	7E	7E	AD
000010E0	13	69	FC	04	03	07	8B	C9	1C	EE	65	E2	6D	06	AD	C8
000010F0	36	6D	25	1A	EC	53	62	C2	2C	76	94	FC	7B	BB	72	F0
00001100	FD	37	D3	26	DC	A4	7A	AA	02	DB	D4	65	38	E0	B6	1B
00001110	C5	08	CA	C7	6B	EA	30	C2	A6	97	C1	8D	76	AA	68	C4
00001120	EC	05	24	AF	83	A4	41	F2	BD	BF	70	CB	5E	2F	D5	BE
00001130	FB	2D	CE	64	51	8F	05	B7	05	53	EB	67	9F	02	18	1C
00001140	FA	20	80	29	FE	B6	99	D9	2A	9C	A1	4E	13	AB	4A	DD
00001150	3C	4C	E6	A3	93	7C	ED	4F	D2	BD	62	F7	02	DE	0B	01
00001160	0A	60	B4	E7	DE	44	C5	D0	CF	11	78	53	BB	50	FF	D2
00001170	18	CB	47	21	68	B3	07	2C	AD	8D	4F	D8	E6	ED	7D	D3
00001180	E8	0A	25	76	82	A5	1D	4A	C0	1F	DD	0F	2C	31	05	53
00001190	E5	72	F3	C9	25	B8	76	B4	86	95	C7	5C	C3	92	8A	E0
000011A0	8B	4E	89	D2	FF	04	E1	2D	E4	16	11	E2	B4	18	E7	4F
000011B0	B3	1C	05	1C	A8	74	F2	AF	AD	A5	A5	73	36	DC	B8	85
000011C0	90	4F	27	AB	AA	03	42	F7	A2	4C	12	11	27	B2	C9	E2
000011D0	B0	5C	C3	E6	AF	B3	5F	D3	D6	39	50	A3	36	01	AE	24
000011E0	CD	32	03	75	75	C2	FF	76	36	30	C4	69	AD	0D	DB	B3
000011F0	17	25	CB	6E	D7	AE	78	A2	7E	81	D5	B1	B0	24	A9	10
00001200	00	10	00	00	00	00	00	00	64	00	00	00	00	00	00	00

Figure 43

Case 2 – File size > 5244992 bytes (approximately 5MB)

In this case, only half of the file is alternatively encrypted:



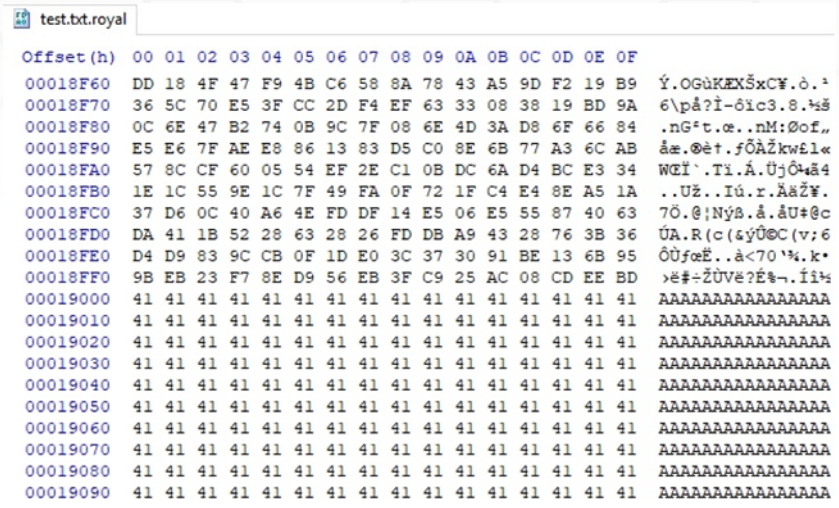
test2.txt.royal

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
005007E0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
005007F0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
00500800	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
00500810	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
00500820	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
00500830	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
00500840	41	20	EB	FA	E2	A3	01	00	00	90	AD	F7	E2	A3	01	00	A ëúâ£.....÷â£..
00500850	1D	9C	BE	8F	83	60	D6	7F	3E	11	EF	C4	F7	EF	F1	14	.œ¾.ƒ`Ö.>.ïÄ÷ïñ.
00500860	71	E4	4F	35	E7	B2	CF	72	C6	9A	11	7E	AA	03	30	69	qäO5ç²ÏrÆš.~ª.0i
00500870	CE	BA	B9	F3	7D	7D	27	7D	32	B7	D4	5C	FE	32	EC	11	Î°¹ó}}'}2·Ô\þ2ì.
00500880	83	1A	B9	76	6F	E0	1F	2D	69	2D	51	2A	94	B5	ED	4A	ƒ.¹voà.-i-Q*"µíJ
00500890	41	5E	D3	24	23	66	0E	D0	21	96	49	B6	0B	98	BC	0E	A^Ó$#f.Ð!–I¶.˜¼.
005008A0	0B	1C	6F	ED	3D	14	92	9D	69	B4	58	2E	36	46	D6	DA	..oí=.'.i´X.6FÖÚ
005008B0	2F	6B	18	94	EA	71	DE	7E	AB	BE	18	57	20	FE	4B	01	/k."êqÞ~«¾.W þK.
005008C0	E4	89	45	02	0F	B6	B4	A3	10	C6	37	01	1E	8F	50	0E	ä‰E..¶´£.Æ7...P.
005008D0	63	B5	C6	05	9B	29	9C	84	2C	4B	15	AF	36	3D	F6	66	cµÆ.›)œ„,K.¯6=öf
005008E0	BE	23	C9	4C	D2	B5	55	D2	A2	74	DF	9E	6C	53	36	D6	¾#ÉLÒµUÒ¢tß.lS6Ö
005008F0	C7	E7	A4	35	5B	DC	7A	3F	D2	2A	FB	0D	96	49	21	A6	Çç¤5[Üz?Ò*û.–I!¦
00500900	8A	E3	37	79	75	D1	49	5E	D4	DE	0C	11	DA	B9	AF	0A	Šã7yuÑI^ÔÞ..Ú¹¯.
00500910	42	8B	98	8D	F5	29	B4	D7	99	49	24	E3	B6	55	41	21	B‹˜.õ)´×™I$ã¶UA!
00500920	C5	83	5C	EF	C5	31	D7	85	58	F5	73	CD	F9	43	92	FA	Åƒ\ïÅ1×…XõsÍùC'ú
00500930	19	E8	E3	15	7A	7E	A5	74	B6	A3	A8	40	94	47	5D	7D	.èã.z~¥t¶£¨@"G]}
00500940	EB	A7	52	3D	78	DC	F9	FA	C4	BA	04	8D	62	FE	44	08	ë§R=xÜùúÄº..bþD.
00500950	12	EE	5A	5B	9E	9E	42	A7	7F	04	22	BB	20	3E	E4	7D	.îZ[žžB§.."» >ä}
00500960	FA	BB	FA	C8	07	DA	32	A6	BC	67	77	BD	9E	00	43	DD	ú»úÈ.Ú2¦¼gw½ž.CÝ
00500970	B2	B1	B0	ED	42	09	B5	54	06	F7	20	1B	A7	43	6A	2E	²±°íB.µT.÷ .§Cj.
00500980	C0	30	F1	37	7D	3D	FE	0B	0E	DA	FB	AD	39	B7	F4	F5	À0ñ7}=þ..Úû.9·ôõ
00500990	67	2F	77	A1	B4	09	8F	E2	F4	E1	54	47	1D	3D	82	2C	g/w¡´..âôáTG.=‚,
005009A0	89	7F	68	B0	1B	8D	A1	BD	44	D0	E4	DF	A6	40	05	D7	‰.h°..¡½DÐäß¦@.×
005009B0	A7	8C	95	03	3C	64	11	7C	B9	48	FB	55	BB	D6	83	86	§Œ•.<d.|¹HûU»Öƒ†
005009C0	31	87	34	D4	D4	A0	13	CC	49	01	E2	25	72	85	65	69	1‡4ÔÔ .ÌI.â%r…ei
005009D0	80	DA	CC	03	FD	FC	7E	E1	58	60	FA	54	11	8B	A5	8F	€ÚÌ.ýü~áX`úT.‹¥.
005009E0	B0	12	C0	6D	BD	AC	3E	DA	AD	09	63	F2	2B	8C	85	A7	°.Àm½¬>Ú..cò+Œ…§
005009F0	52	D4	98	7C	D6	05	93	2C	CB	11	31	20	1A	22	E5	24	RÔ˜|Ö.",Ë.1 ."å$
00500A00	7F	E3	7D	E9	8A	1B	BD	76	D7	BA	60	C0	95	79	F0	52	.ã}éŠ.½v×º`À•yðR
00500A10	46	99	AC	D7	5B	23	01	6D	73	89	C9	D6	45	4F	A0	B7	F™¬×[#.ms‰ÉÖEO ·
00500A20	A4	A7	FA	CA	80	EA	3F	D0	3E	38	28	EA	18	90	C3	89	¤§úÊ€ê?Ð>8(ê..Ã‰
00500A30	27	76	23	21	66	66	40	AB	85	2D	B6	92	37	29	C9	A9	'v#!ff@«…-¶'7)É©
00500A40	1B	B7	1F	08	57	45	81	E6	23	7E	01	2B	F2	BD	7B	B1	.·..WE.æ#~.+ò½{±
00500A50	41	08	50	00	00	00	00	00	32	00	00	00	00	00	00	00	A.P.....2.......

Figure 44

Case 3 – Modify the encryption percentage using the "-ep" parameter

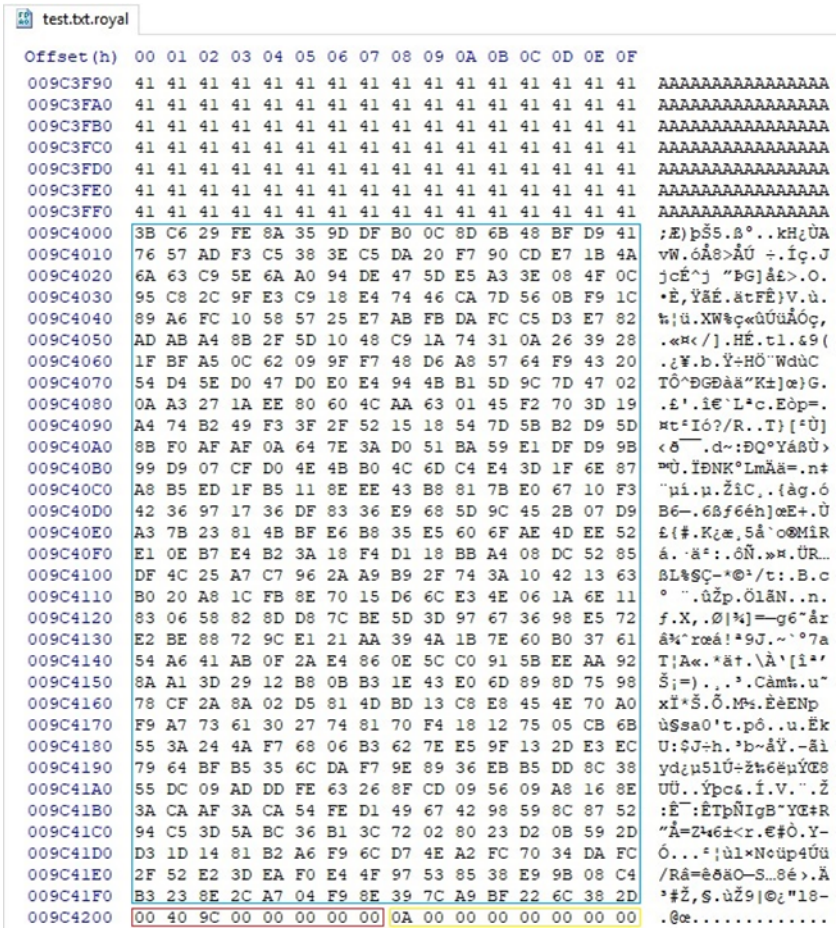
Royal ransomware can modify the percentage of the file content to be encrypted. For example, we've set the "-ep" parameter to 10, and the malware only encrypts 10% of the file, as highlighted below.



test.txt.royal

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00018F60	DD	18	4F	47	F9	4B	C6	58	8A	78	43	A5	9D	F2	19	B9	Ý.OGùKÆXŠxC¥.ò.¹
00018F70	36	5C	70	E5	3F	CC	2D	F4	EF	63	33	08	38	19	BD	9A	6\på?Ì-ôïc3.8.½š
00018F80	0C	6E	47	B2	74	0B	9C	7F	08	6E	4D	3A	D8	6F	66	84	.nG²t.œ..nM:Øof„
00018F90	E5	E6	7F	AE	E8	86	13	83	D5	C0	8E	6B	77	A3	6C	AB	åæ.®è†.ƒÕÀŽkw£l«
00018FA0	57	8C	CF	60	05	54	EF	2E	C1	0B	DC	6A	D4	BC	E3	34	WŒÏ`.Tï.Á.ÜjÔ¼ã4
00018FB0	1E	1C	55	9E	1C	7F	49	FA	0F	72	1F	C4	E4	8E	A5	1A	..Už..Iú.r.ÄäŽ¥.
00018FC0	37	D6	0C	40	A6	4E	FD	DF	14	E5	06	E5	55	87	40	63	7Ö.@¦Nýß.å.åU‡@c
00018FD0	DA	41	1B	52	28	63	28	26	FD	DB	A9	43	28	76	3B	36	ÚA.R(c(&ýÛ©C(v;6
00018FE0	D4	D9	83	9C	CB	0F	1D	E0	3C	37	30	91	BE	13	6B	95	ÔÙƒœË..à<70'¾.k•
00018FF0	9B	EB	23	F7	8E	D9	56	EB	3F	C9	25	AC	08	CD	EE	BD	›ë#÷ŽÙVë?É%¬.Íî½
00019000	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
00019010	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
00019020	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
00019030	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
00019040	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
00019050	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
00019060	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
00019070	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
00019080	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
00019090	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA

Figure 45



test.txt.royal

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
009C3F90	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
009C3FA0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
009C3FB0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
009C3FC0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
009C3FD0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
009C3FE0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
009C3FF0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
009C4000	3B	C6	29	FE	8A	35	9D	DF	B0	0C	8D	6B	48	BF	D9	41	;Æ)þŠ5.ß°..kH¿ÙA
009C4010	76	57	AD	F3	C5	38	3E	C5	DA	20	F7	90	CD	E7	1B	4A	vW.óÅ8>ÅÚ ÷.Íç.J
009C4020	6A	63	C9	5E	6A	A0	94	DE	47	5D	E5	A3	3E	08	4F	0C	jcÉ^j "ÞG]å£>.O.
009C4030	95	C8	2C	9F	E3	C9	18	E4	74	46	CA	7D	56	0B	F9	1C	•È,ŸãÉ.ätFÊ}V.ù.
009C4040	89	A6	FC	10	58	57	25	E7	AB	FB	DA	FC	C5	D3	E7	82	‰¦ü.XW%ç«ûÚüÅÓç,
009C4050	AD	AB	A4	8B	2F	5D	10	48	C9	1A	74	31	0A	26	39	28	.«¤‹/].HÉ.t1.&9(
009C4060	1F	BF	A5	0C	62	09	9F	F7	48	D6	A8	57	64	F9	43	20	.¿¥.b.Ÿ÷HÖ¨WdùC
009C4070	54	D4	5E	D0	47	D0	E0	E4	94	4B	B1	5D	9C	7D	47	02	TÔ^ÐGÐàä"K±]œ}G.
009C4080	0A	A3	27	1A	EE	80	60	4C	AA	63	01	45	F2	70	3D	19	.£'.î€`Lªc.Eòp=.
009C4090	A4	74	B2	49	F3	3F	2F	52	15	18	54	7D	5B	B2	D9	5D	¤t²Ió?/R..T}[²Ù]
009C40A0	8B	F0	AF	AF	0A	64	7E	3A	D0	51	BA	59	E1	DF	D9	9B	‹ð¯¯.d~:ÐQºYáßÙ›
009C40B0	99	D9	07	CF	D0	4E	4B	B0	4C	6D	C4	E4	3D	1F	6E	87	™Ù.ÏÐNK°LmÄä=.n‡
009C40C0	A8	B5	ED	1F	B5	11	8E	EE	43	B8	81	7B	E0	67	10	F3	¨µí.µ.ŽîC¸.{àg.ó
009C40D0	42	36	97	17	36	DF	83	36	E9	68	5D	9C	45	2B	07	D9	B6—.6ßƒ6éh]œE+.Ù
009C40E0	A3	7B	23	81	4B	BF	E6	B8	35	E5	60	6F	AE	4D	EE	52	£{#.K¿æ¸5å`o®MîR
009C40F0	E1	0E	B7	E4	B2	3A	18	F4	D1	18	BB	A4	08	DC	52	85	á.·ä²:.ôÑ.»¤.ÜR…
009C4100	DF	4C	25	A7	C7	96	2A	A9	B9	2F	74	3A	10	42	13	63	ßL%§Ç–*©¹/t:.B.c
009C4110	B0	20	A8	1C	FB	8E	70	15	D6	6C	E3	4E	06	1A	6E	11	° ¨.ûŽp.ÖlãN..n.
009C4120	83	06	58	82	8D	D8	7C	BE	5D	3D	97	67	36	98	E5	72	ƒ.X‚.Ø|¾]=—g6˜år
009C4130	E2	BE	88	72	9C	E1	21	AA	39	4A	1B	7E	60	B0	37	61	â¾ˆrœá!ª9J.~`°7a
009C4140	54	A6	41	AB	0F	2A	E4	86	0E	5C	C0	91	5B	EE	AA	92	T¦A«.*ä†.\À'[îª'
009C4150	8A	A1	3D	29	12	B8	0B	B3	1E	43	E0	6D	89	8D	75	98	Š¡=).¸.³.Càm‰.u˜
009C4160	78	CF	2A	8A	02	D5	81	4D	BD	13	C8	E8	45	4E	70	A0	xÏ*Š.Õ.M½.ÈèENp
009C4170	F9	A7	73	61	30	27	74	81	70	F4	18	12	75	05	CB	6B	ù§sa0't.pô..u.Ëk
009C4180	55	3A	24	4A	F7	68	06	B3	62	7E	E5	9F	13	2D	E3	EC	U:$J÷h.³b~åŸ.-ãì
009C4190	79	64	BF	B5	35	6C	DA	F7	9E	89	36	EB	B5	DD	8C	38	yd¿µ5lÚ÷ž‰6ëµÝŒ8
009C41A0	55	DC	09	AD	DD	FE	63	26	8F	CD	09	56	09	A8	16	8E	UÜ..Ýþc&.Í.V.¨.Ž
009C41B0	3A	CA	AF	3A	CA	54	FE	D1	49	67	42	98	59	8C	87	52	:Ê¯:ÊTþÑIgB˜YŒ‡R
009C41C0	94	C5	3D	5A	BC	36	B1	3C	72	02	80	23	D2	0B	59	2D	"Å=Z¼6±<r.€#Ò.Y-
009C41D0	D3	1D	14	81	B2	A6	F9	6C	D7	4E	A2	FC	70	34	DA	FC	Ó...²¦ùl×N¢üp4Úü
009C41E0	2F	52	E2	3D	EA	F0	E4	4F	97	53	85	38	E9	9B	08	C4	/Râ=êðäO—S…8é›.Ä
009C41F0	B3	23	8E	2C	A7	04	F9	8E	39	7C	A9	BF	22	6C	38	2D	³#Ž,§.ùŽ9|©¿"l8-
009C4200	00	40	9C	00	00	00	00	00	0A	00	00	00	00	00	00	00	.@œ.....

Figure 46

Indicators of Compromise

SHA256

f484f919ba6e36ff33e4fb391b8859a94d89c172a465964f99d6113b55ced429

Royal Ransom Note

README.txt

Process spawned

C:\Windows\System32\vssadmin.exe delete shadows /all /quiet