

A Technical Analysis of Royal Ransomware

Prepared by: Vlad Pasca, Senior Malware &
Threat Analyst



[SecurityScorecard.com](https://www.SecurityScorecard.com)
info@securityscorecard.com

Tower 49
12 E 49th Street
Suite 15-001
New York, NY 10017
[1.800.682.1707](tel:18006821707)

Table of contents

Executive summary	2
Analysis and findings	2
Thread activity – StartAddress function	7
Thread activity – sub_7FF668CDF870 function	8
Case 1 – File size < 5244992 bytes (approximately 5MB)	12
Case 2 – File size > 5244992 bytes (approximately 5MB)	13
Case 3 – Modify the encryption percentage using the “-ep” parameter	14
Indicators of Compromise	16

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:

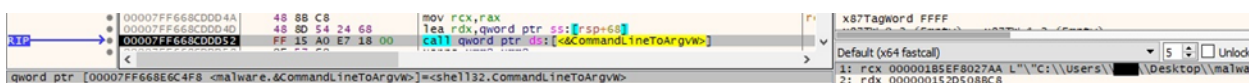


Figure 2

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).

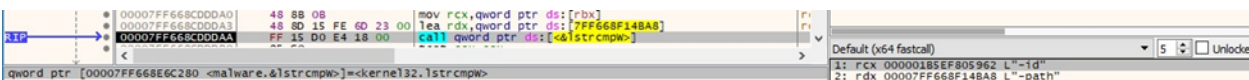


Figure 3

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

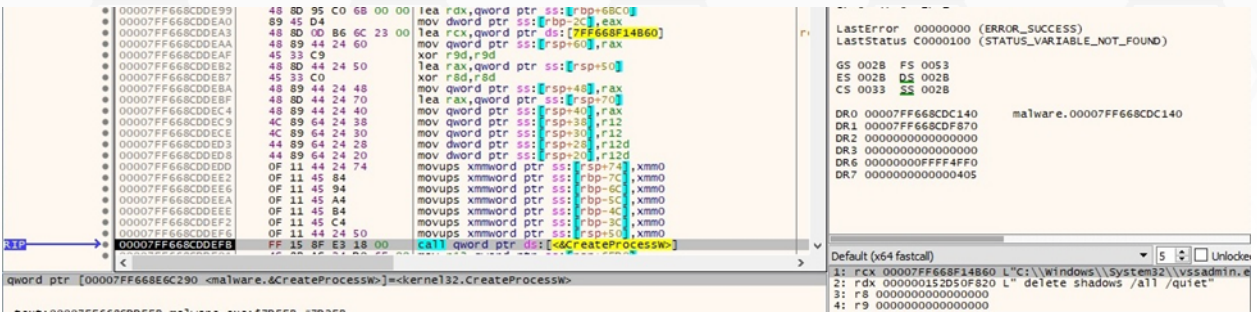


Figure 4

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
- perlogs
- mozilla
- tor browser
- boot
- \$windows.~ws
- \$windows.~bt
- windows.old

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



Figure 5

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

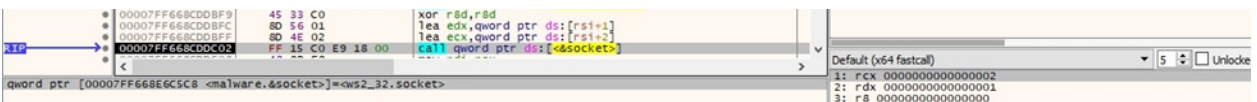


Figure 6

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

```

00007FF668CDDC11 48 89 74 24 40 mov qword ptr ss:[rsp+40],rsi
00007FF668CDDC16 48 8D 4C 24 60 lea rcx,qword ptr ss:[rsp+60]
00007FF668CDDC1B 48 89 74 24 38 mov qword ptr ss:[rsp+38],rsi
00007FF668CDDC20 48 80 83 18 60 00 00 lea rax,qword ptr ds:[rbx+6018]
00007FF668CDDC27 48 89 4C 24 30 mov qword ptr ss:[rsp+30],rcx
00007FF668CDDC2C 44 8D 4E 10 lea r9d,qword ptr ds:[rsi+10]
00007FF668CDDC30 C7 44 24 28 08 00 00 mov dword ptr ss:[rsp+28],8
00007FF668CDDC38 4C 8D 44 24 50 lea r8,qword ptr ss:[rsp+50]
00007FF668CDDC3D 48 8B CF mov rcx,rdi
00007FF668CDDC40 48 89 44 24 20 mov qword ptr ss:[rsp+20],rax
00007FF668CDDC45 8A 06 00 00 CB mov edx,C8000006
00007FF668CDDC4A C7 44 24 50 B9 07 A2 mov dword ptr ss:[rsp+50],25A207B9
00007FF668CDDC52 C7 44 24 54 F3 D0 60 mov dword ptr ss:[rsp+54],4660DDF3
00007FF668CDDC5A C7 44 24 58 E8 E9 76 mov dword ptr ss:[rsp+58],E576E98E
00007FF668CDDC62 C7 44 24 5C BC 74 06 mov dword ptr ss:[rsp+5C],3E06748C
RIP 00007FF668CDDC6A FF 15 38 E9 18 00 call qword ptr ds:[&WSALoctl]
qword ptr [00007FF668E6C5A8 <malware.&WSALoctl>]=&ws2_32.WSALoctl>

```

Figure 7

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

```

00007FF668CDFD18 48 8D 4C 24 30 lea rcx,qword ptr ss:[rsp+30]
RIP 00007FF668CDFD1D FF 15 15 C4 18 00 call qword ptr ds:[&GetNativeSystemInfo]
qword ptr [00007FF668E6C138 <malware.&GetNativeSystemInfo>]=&kernel32.GetNativeSystemInfo>

```

Figure 8

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

```

00007FF668CDFD41 48 89 6C 24 28 mov qword ptr ss:[rsp+28],rbp
00007FF668CDFD46 4C 8D 05 23 FF FF FF lea r8,qword ptr ds:[?FF668CDF870]
00007FF668CDFD4D 4C 8B CF mov r9,rdi
00007FF668CDFD50 89 6C 24 20 mov dword ptr ss:[rsp+20],ebp
00007FF668CDFD54 33 D2 xor edx,edx
00007FF668CDFD5E 33 C9 xor ecx,ecx
RIP 00007FF668CDFD5B FF 15 8A C5 18 00 call qword ptr ds:[&CreateThread]
qword ptr [00007FF668E6C2E8 <malware.&CreateThread>]=&kernel32.CreateThread>

```

Figure 9

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

```

00007FF668CDDC1D9 48 89 6C 24 28 mov qword ptr ss:[rsp+28],rbp
00007FF668CDDC1DE 4C 8D 05 58 FF FF FF lea r8,qword ptr ds:[?FF668CDDC140]
00007FF668CDDC1E3 4C 8B CE mov r9,rsi
00007FF668CDDC1EB 89 6C 24 20 mov dword ptr ss:[rsp+20],ebp
00007FF668CDDC1EC 33 D2 xor edx,edx
00007FF668CDDC1EE 33 C9 xor ecx,ecx
RIP 00007FF668CDDC1F0 FF 15 F2 00 19 00 call qword ptr ds:[&CreateThread]
qword ptr [00007FF668E6C2E8 <malware.&CreateThread>]=&kernel32.CreateThread>

```

Figure 10

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

```

00007FF668CDEB48 45 33 C0 xor r8d,r8d
00007FF668CDEB4B 48 8D 54 24 40 lea rdx,qword ptr ss:[rsp+40]
00007FF668CDEB50 48 8B C8 mov rcx,rax
RIP 00007FF668CDEB53 FF 15 67 D5 18 00 call qword ptr ds:[&GetIpAddrTable]
qword ptr [00007FF668E6C0C0 <malware.&GetIpAddrTable>]=&iphlpapi.GetIpAddrTable>

```

Figure 11

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

```

RIP → 00007FF668CDE93E 8B CB mov ecx,ebx
00007FF668CDE93E FF 15 94 D9 18 00 call qword ptr ds:[<antohl>]
qword ptr [00007FF668E6C5D8 <malware.&antohl>]=<aws2_32.ntohl>

```

Figure 12

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

```

RIP → 00007FF668CDE775 33 D2 xor edx,edx
00007FF668CDE777 48 8B F1 mov rsi,rcx
00007FF668CDE77A 41 89 01 00 00 00 mov r9d,i
00007FF668CDE780 45 33 C0 xor r8d,r8d
00007FF668CDE783 48 80 4A FF lea rcx,qword ptr ds:[r8d-1]
00007FF668CDE787 FF 15 48 D9 18 00 call qword ptr ds:[<createIoCompletionPort>]
qword ptr [00007FF668E6C0D8 <malware.&createIoCompletionPort>]=<kernel32.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):

```

RIP → 00007FF668CDE984 45 33 C9 xor r9d,r9d
00007FF668CDE987 C7 44 24 28 01 00 00 mov dword ptr ss:[rsp+28],1
00007FF668CDE98F 44 89 7C 24 20 mov dword ptr ss:[rsp+20],r15d
00007FF668CDE994 48 8B 08 mov rcx,qword ptr ds:[rax]
00007FF668CDE997 41 8D 51 01 lea edx,qword ptr ds:[r9+1]
00007FF668CDE99B 45 8D 41 06 lea r8d,qword ptr ds:[r9+6]
00007FF668CDE99F 44 8B 71 10 mov r14d,qword ptr ds:[rcx+10]
00007FF668CDE9A3 41 8B CC mov ecx,r12d
00007FF668CDE9A6 FF 15 14 DC 18 00 call qword ptr ds:[<wSocketw>]
qword ptr [00007FF668E6C5C0 <malware.&wSocketw>]=<ws2_32.WSASocketw>

```

Figure 14

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

```

RIP → 00007FF668CDE9B9 41 8B 10 00 00 00 mov r8d,10
00007FF668CDE9BF 4C 89 64 24 40 mov qword ptr ss:[rsp+40],r12
00007FF668CDE9C4 48 8D 54 24 40 lea rdx,qword ptr ss:[rsp+40]
00007FF668CDE9C8 48 8B C8 mov rcx,rax
00007FF668CDE9CC FF 15 CE DB 18 00 call qword ptr ds:[<bind>]
qword ptr [00007FF668E6C5A0 <malware.&bind>]=<ws2_32.bind>

```

Figure 15

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

```

RIP → 00007FF668CDE9DD 48 8B 13 mov rdx,qword ptr ds:[rdx]
00007FF668CDE9E0 45 33 C9 xor r9d,r9d
00007FF668CDE9E3 45 33 C0 xor r8d,r8d
00007FF668CDE9E6 FF 15 EC D6 18 00 call qword ptr ds:[<createIoCompletionPort>]
qword ptr [00007FF668E6C0D8 <malware.&createIoCompletionPort>]=<kernel32.CreateIoCompletionPort>

```

Figure 16

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

Figure 17

Time	Process Name	PID	Operation	Path	Result	Detail	TID
8:18.5	malware.exe	4460	TCP Reconnect	192.168.164.128:50179->192.168.164.0:445	SUCCESS	Length: 0, seqn...	0
8:19.0	malware.exe	4460	TCP Reconnect	192.168.164.128:50179->192.168.164.0:445	SUCCESS	Length: 0, seqn...	0
8:19.3	malware.exe	4460	TCP Reconnect	192.168.164.128:50180->192.168.164.1:445	SUCCESS	Length: 0, seqn...	0
8:19.5	malware.exe	4460	TCP Reconnect	192.168.164.128:50181->192.168.164.2:445	SUCCESS	Length: 0, seqn...	0
8:19.5	malware.exe	4460	TCP Disconnect	192.168.164.128:50433->192.168.164.255:445	SUCCESS	Length: 0, seqn...	0
8:20.0	malware.exe	4460	TCP Reconnect	192.168.164.128:50181->192.168.164.2:445	SUCCESS	Length: 0, seqn...	0
8:20.0	malware.exe	4460	TCP Reconnect	192.168.164.128:50182->192.168.164.3:445	SUCCESS	Length: 0, seqn...	0
8:20.0	malware.exe	4460	TCP Reconnect	192.168.164.128:50183->192.168.164.4:445	SUCCESS	Length: 0, seqn...	0
8:20.0	malware.exe	4460	TCP Reconnect	192.168.164.128:50184->192.168.164.5:445	SUCCESS	Length: 0, seqn...	0
8:20.0	malware.exe	4460	TCP Reconnect	192.168.164.128:50185->192.168.164.6:445	SUCCESS	Length: 0, seqn...	0
8:20.0	malware.exe	4460	TCP Reconnect	192.168.164.128:50186->192.168.164.7:445	SUCCESS	Length: 0, seqn...	0
8:20.0	malware.exe	4460	TCP Reconnect	192.168.164.128:50187->192.168.164.8:445	SUCCESS	Length: 0, seqn...	0
8:20.0	malware.exe	4460	TCP Reconnect	192.168.164.128:50188->192.168.164.9:445	SUCCESS	Length: 0, seqn...	0
8:20.0	malware.exe	4460	TCP Reconnect	192.168.164.128:50189->192.168.164.10:445	SUCCESS	Length: 0, seqn...	0
8:20.0	malware.exe	4460	TCP Reconnect	192.168.164.128:50190->192.168.164.11:445	SUCCESS	Length: 0, seqn...	0
8:20.0	malware.exe	4460	TCP Reconnect	192.168.164.128:50191->192.168.164.12:445	SUCCESS	Length: 0, seqn...	0
8:20.0	malware.exe	4460	TCP Reconnect	192.168.164.128:50192->192.168.164.13:445	SUCCESS	Length: 0, seqn...	0
8:20.0	malware.exe	4460	TCP Reconnect	192.168.164.128:50193->192.168.164.14:445	SUCCESS	Length: 0, seqn...	0

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\$":

```

00007FF668CDE5CE 4C 8D 44 24 68 lea r8,qword ptr ss:[rsp+68]
00007FF668CDE5D3 48 8D 44 24 7C lea rax,qword ptr ss:[rsp+7C],ebx
00007FF668CDE5D8 89 5C 24 7C mov dword ptr ss:[rsp+7C],ebx
00007FF668CDE5DC 48 89 44 24 28 mov qword ptr ss:[rsp+28],rax
00007FF668CDE5E1 48 8D 4D 90 lea rax,qword ptr ss:[rbp-70]
00007FF668CDE5E5 48 8D 44 24 70 lea rax,qword ptr ss:[rsp+70]
00007FF668CDE5EA 89 5C 24 78 mov dword ptr ss:[rsp+78],ebx
00007FF668CDE5EE 41 89 FF FF FF mov r9d,FFFFFFFF
00007FF668CDE5F4 48 89 44 24 20 mov qword ptr ss:[rsp+20],rax
00007FF668CDE5F9 BA 01 00 00 00 mov edx,1
00007FF668CDE5FE 48 89 5C 24 68 mov qword ptr ss:[rsp+68],rbx
00007FF668CDE603 FF 15 A7 DE 18 00 call qword ptr ds:[<GetShareEnum>]

```

Figure 21

Thread activity – StartAddress function

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

```

00007FF668CDE377 FF 15 B8 01 19 00 call qword ptr ds:[<GetLogicalDrives>]

```

Figure 22

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

```

00007FF668CDE7E2 FF 15 10 FC 18 00 call qword ptr ds:[<CreateFile>]

```

Figure 23

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

```

00007FF668CDE0F4 FF 15 06 FB 18 00 call qword ptr ds:[<WriteFile>]

```

```

Address Hex ASCII
00000074D66FE980 48 65 6C 6C 6F 21 00 0A 0D 0A 09 49 66 20 79 6F Hello!...If yo
00000074D66FE990 75 20 61 72 65 20 72 65 61 64 69 6E 67 20 74 68 u are reading th
00000074D66FE9A0 69 73 2C 20 69 74 20 60 65 61 6E 73 20 74 68 61 is, it means th
00000074D66FE9B0 74 20 79 6F 75 72 20 73 79 73 74 65 60 20 77 65 t, your system we
00000074D66FE9C0 72 65 20 68 69 74 20 62 79 20 52 6F 79 61 6C 20 re hit by Royal
00000074D66FE9D0 72 61 6E 73 6F 6D 77 61 72 65 2E 0D 0A 09 50 6C ransomware...P!
00000074D66FE9E0 65 61 73 65 20 63 6F 6E 74 61 69 74 20 75 73 20 ease contact us
00000074D66FE9F0 76 69 61 20 3A 0D 0A 09 68 74 74 70 3A 2F 2F 72 via :...http://p
00000074D66FEA00 6F 79 61 6C 32 78 74 68 69 67 33 6F 75 35 68 64 oyal2xth1g30u5h/
00000074D66FEA10 6A 65 6C 61 78 74 6E 69 32 6E 79 61 64 36 64 70 delaxtn12yadddp
00000074D66FEA20 6D 70 78 65 64 69 64 2E 6F 6E 69 6F 6E 2F 41 41 mpxed1d.onion/AA
00000074D66FEA30 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAB
00000074D66FEA40 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 BBBBBBBBBBBBBBBB...
00000074D66FEA50

```

Figure 24

The ransomware starts enumerating the files using the FindFirstFileW function:

```

00007FF668CDE467 FF 15 B8 FF 18 00 call qword ptr ds:[<FindFirstFileW>]

```

Figure 25

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

```
00007FF668CDC68A 48 8B 12 mov rdx,qword ptr ds:[rdx]
00007FF668CDC68D 48 8B 78 18 08 cmp qword ptr ds:[rbx+18],8
00007FF668CDC692 48 8B C8 mov rcx,rbx
00007FF668CDC695 72 03 jz malware.7FF668CDC69A
00007FF668CDC697 48 8B 08 mov rcx,qword ptr ds:[rbx]
00007FF668CDC69A FF 15 68 FE 18 00 call qword ptr ds:[&StrStrIW]
```

Figure 26

The files enumeration continues by calling the FindNextFileW API:

```
00007FF668CDBF68 49 8D 55 38 lea rdx,qword ptr ds:[r13+38]
00007FF668CDBF6F 49 8B 4D 30 mov rcx,qword ptr ds:[r13+30]
00007FF668CDBF73 FF 15 9F 04 19 00 call qword ptr ds:[&FindNextFileW]
```

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+49fo
; sub_7FF668CDF870+59fo ...
db 'MIICCAKAgEAuIFX+pJCUCk9xsWLVHpCpw6TL20HG/Vk4vF3GY1r6H1tX7BMRFA',0Ah
db '7oGyMztNb37xW66NX+uxHghrX3+sm23yJmSfressJIG0vDNZV080JevZxuhHUome',0Ah
db 'RdLfjRYpuEg8mbEdL1c1jQqoEZEh0Ib8Lhv1dBDnwXEBGnf/k8uMuY784xxDfbpt',0Ah
db 'SB1500HRfvIqMcIbskQ8RfMDFeiwYNRVrCkyhXOTB+RkmzTtp7q8gjnA1AHOfHSx',0Ah
db 'e0BVt9Lz27uuS4RIf/b31aiBoLzAWft44wSC4diYvSom93d6S2K6oMYNOQvSu+zI',0Ah
db 'U8/yzxebDN0bWJLVPZxndQFBVHiTXQfWDi1BdsalJR2BHPj/tYwd4j/72vN1vywt',0Ah
db 'M3sn5TJNq1/gJZ7HuU0QOyBzdLk3vpmmqby5wwXLd+WKPWv3HEKaOy80K0F7FrhC',0Ah
db '0g3nbKAF5Y+MzkEUNHDvwTk9uKY6ILCJ0/fXE78ULcxrgy0w76WVZlweLrsVun5k',0Ah
db 'J9i+LhcBNH7DJGJ544zC1yF1s8geW00VYCh7Ur4o0aE2EwTNYeLIgsFf4A6m0E0',0Ah
db '6gfoRDNH40U4DdK5JFQRp2tLXI93o7hSEEAHJe7s0LyD1DLXksQjNkRUE+0jd5G',0Ah
db 'AGdM3G7RZuWrMC4FfmtPlzYfd15o2k/u9RYi7fi8pu34GQvvpPhW8wK8CAQM=',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+60to
; sub_7FF668CDFE50+189to ...

align 8
aCryptoRsaRsaCr db 'crypto\rsa\rsa_crpt.c',0
; DATA XREF: sub_7FF668CDFE50+6Cto
; sub_7FF668CDFE50+195to ...

align 10h
aCryptoBioBioli db 'crypto\bio\bio_lib.c',0
; DATA XREF: sub_7FF668CE0150+13Dto
; sub_7FF668CE02F0+139to ...

align 8
aBioNewEx db 'BIO_new_ex',0
; DATA XREF: sub_7FF668CE0C70+36to
; sub_7FF668CE0C70+B2to ...

align 8
aBioReadIntern db 'bio_read_intern',0
; DATA XREF: sub_7FF668CE13F0+2Cto
; sub_7FF668CE13F0+FDto ...

aBioWriteIntern db 'bio_write_intern',0
; DATA XREF: sub_7FF668CE1600+CEto
; sub_7FF668CE1600+1DDto ...

align 20h
aBioPuts db 'BIO_puts',0
; DATA XREF: sub_7FF668CE0990+168to
; sub_7FF668CE0990+203to ...

align 10h
aBioGets db 'BIO_gets',0
; DATA XREF: sub_7FF668CE06F0+32to
; sub_7FF668CE06F0+8Dto ...

align 4
asc_7FF668E6C7DC db ' ',0
; DATA XREF: sub_7FF668CE0990+84to
; sub_7FF668CE0990+B4to ...

align 20h
aBioCtrl db 'BIO_ctrl',0
; DATA XREF: sub_7FF668CE02F0+12Dto

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**):


```

.text:00007FF668C610D1 movzx esi, al
.text:00007FF668C610D4 movzx edi, bl
.text:00007FF668C610D7 movzx ebp, cl
.text:00007FF668C610DA movzx r10d, byte ptr [r14+rsi*8+2]
.text:00007FF668C610E0 movzx r11d, byte ptr [r14+rdi*8+2]
.text:00007FF668C610E6 movzx r12d, byte ptr [r14+rbp*8+2]
.text:00007FF668C610EC movzx esi, dl
.text:00007FF668C610EF movzx edi, bh
.text:00007FF668C610F2 movzx ebp, ch
.text:00007FF668C610F5 movzx r8d, byte ptr [r14+rsi*8+2]
.text:00007FF668C610FB mov edi, [r14+rdi*8]
.text:00007FF668C610FF mov ebp, [r14+rbp*8]
.text:00007FF668C61103 and edi, 0FF00h
.text:00007FF668C61109 and ebp, 0FF00h
.text:00007FF668C6110F xor r10d, edi
.text:00007FF668C61112 xor r11d, ebp
.text:00007FF668C61115 shr ecx, 10h
.text:00007FF668C61118 movzx esi, dh
.text:00007FF668C6111B movzx edi, ah
.text:00007FF668C6111E shr edx, 10h
.text:00007FF668C61121 mov esi, [r14+rsi*8]
.text:00007FF668C61125 mov edi, [r14+rdi*8]
.text:00007FF668C61129 and esi, 0FF00h
.text:00007FF668C6112F and edi, 0FF00h
.text:00007FF668C61135 shr ebx, 10h
.text:00007FF668C61138 xor r12d, esi
.text:00007FF668C6113B xor r8d, edi
.text:00007FF668C6113E shr eax, 10h
.text:00007FF668C61141 movzx esi, cl
.text:00007FF668C61144 movzx edi, dl
.text:00007FF668C61147 movzx ebp, al
.text:00007FF668C6114A mov esi, [r14+rsi*8]
.text:00007FF668C6114E mov edi, [r14+rdi*8]
.text:00007FF668C61152 mov ebp, [r14+rbp*8]
.text:00007FF668C61156 and esi, 0FF0000h
.text:00007FF668C6115C and edi, 0FF0000h
.text:00007FF668C61162 and ebp, 0FF0000h
.text:00007FF668C61168 xor r10d, esi
.text:00007FF668C6116B xor r11d, edi
.text:00007FF668C6116E xor r12d, ebp
.text:00007FF668C61171 movzx esi, bl
.text:00007FF668C61174 movzx edi, dh

```

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:

```

mov dword ptr ss:[rsp+58],edi
add rdx,r15
mov qword ptr ss:[rsp+20],rdi
lea r9,qword ptr ss:[rsp+58]
mov rcx,r14
call qword ptr ds:[<writefile>]

```

qword ptr [00007FF668C6410 <malware.&writefile>]=<kernel32.writefile>

```

.text:00007FF668CDF6CC malware.exe:$7F6CC #7EACC

```

Figure 38

```

mov r8d,200
mov dword ptr ss:[rsp+50],edi
lea rdx,qword ptr ss:[rbp+30]
mov qword ptr ss:[rsp+20],rdi
sub r8d,ebx
lea r9,qword ptr ss:[rsp+50]
add rdx,ax
mov rcx,r14
call qword ptr ds:[<writefile>]

```

qword ptr [00007FF668C6410 <malware.&writefile>]=<kernel32.writefile>

```

.text:00007FF668CDF765 malware.exe:$7F765 #7EB65

```

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 !..Ofcâuè.i!Ö.ÄÄ
00000FD0 2A 08 0F C0 85 18 2A 01 1C A9 BA 40 29 27 1C 0F *..Ä...*..°@)'..
00000FE0 8C 61 25 E6 A5 A8 F7 B1 D3 01 66 20 09 16 22 AE @a%æ#"+iö.f .."@
00000FF0 FE EA 28 66 CB E5 94 3F 83 48 32 A2 6F F1 D0 A6 pè(frÄÄ"?fh2coñD;
00001000 8D 10 8F 88 B5 42 B4 61 81 6B 70 D2 A3 B5 53 AD ...~µB'a.kpÖ£µS.
00001010 9A 0A DE 50 94 F1 AA ED 4E 8C ED C1 87 12 83 7C š.PP"ñ"iNGiÄ+.f|
00001020 73 0A 36 51 17 AC 76 DD FB B3 EE 5C FB 0B 5D D6 s.6Q.-vÝú'i\ù.]Ö
00001030 10 B3 9D 6F 3B FA 66 60 FC 47 4B 78 44 9C C2 32 .°.o;úf`ùGKxDœÄ2
00001040 98 76 1F 0C FE E4 A5 AA 85 C6 A9 39 47 1A B5 28 ~v..pä¥#...E@9G.µ(
00001050 D4 35 A6 44 14 18 40 6A EF 1A AA F8 17 A0 09 8B Ô5;D..@jî.°ø. .<
00001060 88 B4 68 0E B3 31 33 53 F4 F3 C3 6E 3A 62 20 89 ^`h.'l3SöóÄn:b %
00001070 87 15 47 48 DB D8 4A A6 FC 12 BE 35 0F 9B B5 4A +.GHÛÖJ;ü.%5.µJ
00001080 E0 E2 92 61 22 64 89 6B CB F0 21 D7 87 F6 45 B2 ää'a"dtkEö!x+öE²
00001090 6F 2A 97 CF 92 73 B8 2B B2 C7 86 E9 CA 98 0D 83 o*-i's,+²ÇtéË".f
000010A0 3F C5 0B 5C C9 7E 63 82 1C F2 46 7E CA CA 6C 31 ?Ä.\É~c,.òF~ÈÉll
000010B0 97 E0 08 59 5D B5 4E B4 02 3E 8D AA D3 FF 25 2B -à.Y|µN'.>.'Óý%+
000010C0 E3 93 69 1D 9E F2 29 85 1E A7 E5 2D D2 0A A1 1D ä"i.žò)....Sä-Ö.ij.
000010D0 50 C5 DA A1 BA F5 F3 6C A9 05 12 46 DE 7E 7E AD PÄÚ;°öó1@..Fp~.
000010E0 13 69 FC 04 03 07 8B C9 1C EE 65 E2 6D 06 AD C8 .iü...<É.íeám..È
000010F0 36 6D 25 1A EC 53 62 C2 2C 76 94 FC 7B BB 72 F0 6m%.iSbÄ,v"ü{>rö
00001100 FD 37 D3 26 DC A4 7A AA 02 DB D4 65 38 E0 B6 1B ý7ó&Ühz².ÛÖešäq.
00001110 C5 08 CA C7 6B EA 30 C2 A6 97 C1 8D 76 AA 68 C4 Ä.ÊÇkè0Ä!-Ä.v²hÄ
00001120 EC 05 24 AF 83 A4 41 F2 BD BF 70 CB 5E 2F D5 BE ì.Ş~fµAò%çpË~/Ö%
00001130 FB 2D CE 64 51 8F 05 B7 05 53 EB 67 9F 02 18 1C ù-ÍdQ...SëgÝ...
00001140 FA 20 80 29 FE B6 99 D9 2A 9C A1 4E 13 AB 4A DD ú €)pË"Ü°æ;N.«JÝ
00001150 3C 4C E6 A3 93 7C ED 4F D2 BD 62 F7 02 DE 0B 01 <Læf"|iOò²sb÷.P..
00001160 0A 60 B4 E7 DE 44 C5 D0 CF 11 78 53 BB 50 FF D2 .`çpDÄÄİ.xS»PÿÖ
00001170 18 CB 47 21 68 B3 07 2C AD 8D 4F D8 E6 ED 7D D3 .EG!h'.,...Oøæi)Ó
00001180 E8 0A 25 76 82 A5 1D 4A C0 1F DD 0F 2C 31 05 53 è.%v,¥.JÄ.Ý.,l.S
00001190 E5 72 F3 C9 25 B8 76 B4 86 95 C7 5C C3 92 8A E0 âróÉ%,v"+Ç\Ä'Šä
000011A0 8B 4E 89 D2 FF 04 E1 2D E4 16 11 E2 B4 18 E7 4F <N%Öy.á-ä..á'.çO
000011B0 B3 1C 05 1C A8 74 F2 AF AD A5 A5 73 36 DC B8 85 '...`tò-.¥¥söÜ,...
000011C0 90 4F 27 AB AA 03 42 F7 A2 4C 12 11 27 B2 C9 E2 .O'«².B÷cL...'²ÉÄ
000011D0 B0 5C C3 E6 AF B3 5F D3 D6 39 50 A3 36 01 AE 24 °\Äæ~³ ÖÖ9P£6.ø$
000011E0 CD 32 03 75 75 C2 FF 76 36 30 C4 69 AD 0D DB B3 Í2.uuÄÿv60Äi..Û²
000011F0 17 25 CB 6E D7 AE 78 A2 7E 81 D5 B1 B0 24 A9 10 .%Ën×@xc~.Ö±°$@.
00001200 00 10 00 00 00 00 00 00 64 00 00 00 00 00 00 00 .....d.....

```

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 AAAAAAAAAAAAAAAAAA
005007F0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAA
00500800 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAA
00500810 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAA
00500820 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAA
00500830 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAA
00500840 41 20 EB FA E2 A3 01 00 00 90 AD F7 E2 A3 01 00 A éú&ε.....+&ε..
00500850 1D 9C BE 8F 83 60 D6 7F 3E 11 EF C4 F7 EF F1 14 .e%4.f'Ö.!.iÄ-iñ.
00500860 71 E4 4F 35 E7 B2 CF 72 C6 9A 11 7E AA 03 30 69 q&05ç'îr&S.~^*.0i
00500870 CE BA B9 F3 7D 7D 27 7D 32 B7 D4 5C FE 32 EC 11 î°:6))')2·Ö\p2i.
00500880 83 1A B9 76 6F E0 1F 2D 69 2D 51 2A 94 B5 ED 4A f.'vo&. -i-Q*~µiJ
00500890 41 5E D3 24 23 66 0E D0 21 96 49 B6 0B 98 BC 0E A^Ó$#t.Đ!-Iq.~4.
005008A0 0B 1C 6F ED 3D 14 92 9D 69 B4 58 2E 36 46 D6 DA ..oi=.'.i'X.6FÖÜ
005008B0 2F 6B 18 94 EA 71 DE 7E AB BE 18 57 20 FE 4B 01 /k."&qB~«%W bpK.
005008C0 E4 89 45 02 0F B6 B4 A3 10 C6 37 01 1E 8F 50 0E &tE..$.f.£.E7...P.
005008D0 63 B5 C6 05 9B 29 9C 84 2C 4B 15 AF 36 3D F6 66 cuE. >)α,,K.~ε=öf
005008E0 BE 23 C9 4C D2 B5 55 D2 A2 74 DF 9E 6C 53 36 D6 %#ÉLÔµUÖct&Z1S6Ö
005008F0 C7 E7 A4 35 5B DC 7A 3F D2 2A FB 0D 96 49 21 A6 Çç&5[Ûz?Ö+ú. -I!;
00500900 8A E3 37 79 75 D1 49 5E D4 DE 0C 11 DA B9 AF 0A Š&7yuNI^ÖB..Ü^~.
00500910 42 8B 98 8D F5 29 B4 D7 99 49 24 E3 B6 55 41 21 B<'·ö) '«~IŞ&âUA!
00500920 C5 83 5C EF C5 31 D7 85 58 F5 73 CD F9 43 92 FA Âf\iÄ1×..XôsîuC'ú
00500930 19 E8 E3 15 7A 7E A5 74 B6 A3 A8 40 94 47 5D 7D .é&.z~ÿtçf"@G}}
00500940 EB A7 52 3D 78 DC F9 FA C4 BA 04 8D 62 FE 44 08 é&R=xÜú&Ä°. .bpD.
00500950 12 EE 5A 5B 9E 9E 42 A7 7F 04 22 BB 20 3E E4 7D .iZ[Z&B$. "» >â)
00500960 FA BB FA C8 07 DA 32 A6 BC 67 77 BD 9E 00 43 DD ú»ú&É.Ü2;4gw&š.Z.CY
00500970 B2 B1 B0 ED 42 09 B5 54 06 F7 20 1B A7 43 6A 2E ±°iB.µT.+ .SCj.
00500980 C0 30 F1 37 7D 3D FE 0B 0E DA FB AD 39 B7 F4 F5 à0ñ7)=p..Üú.9-ôö
00500990 67 2F 77 A1 B4 09 8F E2 F4 E1 54 47 1D 3D 82 2C g/w;'. .â&âTG.=,,
005009A0 89 7F 68 B0 1B 8D A1 BD 44 D0 E4 DF A6 40 05 D7 %..h°. .;:D&â&!@.×
005009B0 A7 8C 95 03 3C 64 11 7C B9 48 FB 55 BB D6 83 86 $E°. <d. |^HúU»Öf+
005009C0 31 87 34 D4 D4 A0 13 CC 49 01 E2 25 72 85 65 69 1+4ÖÖ .II.â&çr...ei
005009D0 80 DA CC 03 FD FC 7E E1 58 60 FA 54 11 8B A5 8F eÜI.yú~âX'út.<¥.
005009E0 B0 12 C0 6D BD AC 3E DA AD 09 63 F2 2B 8C 85 A7 °.Âm&~>Ü..cò+&..S
005009F0 52 D4 98 7C D6 05 93 2C CB 11 31 20 1A 22 E5 24 RÔ~|Ö."É.1 ."â&
00500A00 7F E3 7D E9 8A 1B BD 76 D7 BA 60 C0 95 79 F0 52 .â)é&S.~sv×°`À.y&R
00500A10 46 99 AC D7 5B 23 01 6D 73 89 C9 D6 45 4F A0 B7 F~×[#.m&t&ÉÖEO .
00500A20 A4 A7 FA CA 80 EA 3F D0 3E 38 28 EA 18 90 C3 89 #&ú&é&?Đ>8 (è..Ä&t
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.ε#~.+ô&±(±
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.bt.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.OGùKEXŠxçŸ.ò.š
00018F70	36	5C	70	E5	3F	CC	2D	F4	EF	63	33	08	38	19	BD	9A	è\pâ?î-ôic3.8.šš
00018F80	0C	6E	47	B2	74	0B	9C	7F	08	6E	4D	3A	D8	6F	66	84	.ng*t.e..nm:0of,,
00018F90	E5	E6	7F	AE	E8	86	13	83	D5	C0	8E	6B	77	A3	6C	AB	âe.è†.fôÀžkwèl«
00018FA0	57	8C	CF	60	05	54	EF	2E	C1	0B	DC	6A	D4	BC	E3	34	WCI`.Ti.Á.ÚjÔ4ã4
00018FB0	1E	1C	55	9E	1C	7F	49	FA	0F	72	1F	C4	E4	8E	A5	1A	..Už..Iù.r.ÀãžŸ.
00018FC0	37	D6	0C	40	A6	4E	FD	DF	14	E5	06	E5	55	87	40	63	7ô.è;Nyb.â.âU+@c
00018FD0	DA	41	1B	52	28	63	28	26	FD	DB	A9	43	28	76	3B	36	ÚA.R(c(sýÛ@C(v;6
00018FE0	D4	D9	83	9C	CB	0F	1D	E0	3C	37	30	91	BE	13	6B	95	ÔÛfœÈ...â<70'%.k*
00018FF0	9B	EB	23	F7	8E	D9	56	EB	3F	C9	25	AC	08	CD	EE	BD	>è#-ZÛVe?É*-..íi%>
00019000	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAA
00019010	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAA
00019020	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAA
00019030	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAA
00019040	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAA
00019050	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAA
00019060	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAA
00019070	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAA
00019080	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAA
00019090	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAA

Figure 45

test.bt.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	AAAAAAAAAAAAAAAAAAAA
009C3FA0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAA
009C3FB0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAA
009C3FC0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAA
009C3FD0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAA
009C3FE0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAA
009C3FF0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAA
009C4000	3B	C6	29	FE	8A	35	9D	DF	B0	0C	8D	6B	48	BF	D9	41	;È)þšš.â°.kH¿ÚÀ
009C4010	76	57	AD	F3	C5	38	3E	C5	DA	20	F7	90	CD	E7	1B	4A	vW.óÀš>ÁÛ ÷.íç.J
009C4020	6A	63	C9	5E	6A	A0	94	DE	47	5D	E5	A3	3E	08	4F	0C	jçÉ^j "þG]âè>.O.
009C4030	95	C8	2C	9F	E3	C9	18	E4	74	46	CA	7D	56	0B	F9	1C	*È,ÝÄÈ.štFE)V.ù.
009C4040	89	A6	FC	10	58	57	25	E7	AB	FB	DA	FC	C5	D3	E7	82	ñ;ù.XW*ç«úUúÁÓç,
009C4050	AD	AB	A4	8B	2F	5D	10	48	C9	1A	74	31	0A	26	39	28	««</j.HÉ.tl.š9(
009C4060	1F	BF	A5	0C	62	09	9F	F7	48	D6	A8	57	64	F9	43	20	.¿Ÿ.b.Ý-HÓ-Wdùc
009C4070	54	D4	5E	D0	47	D0	E0	E4	94	4B	B1	5D	9C	7D	47	02	TÔ^ðGðââ"Kz]æ)G.
009C4080	0A	A3	27	1A	EE	80	60	4C	AA	63	01	45	F2	70	3D	19	.è'.ie`L*c.Eòp=.
009C4090	A4	74	B2	49	F3	3F	2F	52	15	18	54	7D	5B	B2	D9	5D	ñt`Ió?/R..T){[?Û]
009C40A0	8B	F0	AF	AF	0A	64	7E	3A	D0	51	BA	59	E1	DF	D9	9B	<è-.d~:ðQ°YâšÛ>
009C40B0	99	D9	07	CF	D0	4E	4B	B0	4C	6D	C4	E4	3D	1F	6E	87	ñÛ.IðNK°LmÁâ=.n+
009C40C0	A8	B5	ED	1F	B5	11	8E	EE	43	B8	81	7B	E0	67	10	F3	ñpi.p.ŽiC.{âg.ó
009C40D0	42	36	97	17	36	DF	83	36	E9	68	5D	9C	45	2B	07	D9	Bè-.èšf6éh]æE+.Û
009C40E0	A3	7B	23	81	4B	BF	E6	B8	35	E5	60	6F	AE	4D	EE	52	è(#.Kçæ.šâ`oðMiR
009C40F0	E1	0E	B7	E4	B2	3A	18	F4	D1	18	BB	A4	08	DC	52	85	â.â*:óÑ.«.ÛR..
009C4100	DF	4C	25	A7	C7	96	2A	A9	B9	2F	74	3A	10	42	13	63	âLšçç-«@*/t:.B.c
009C4110	B0	20	A8	1C	FB	8E	70	15	D6	6C	E3	4E	06	1A	6E	11	°..úžp.ÓlâN..n.
009C4120	83	06	58	82	8D	D8	7C	BE	5D	3D	97	67	36	98	E5	72	f.X.ø Ÿ]—g6"âr
009C4130	E2	BE	88	72	9C	E1	21	AA	39	4A	1B	7E	60	B0	37	61	â%`rœá!*9J.~`°7a
009C4140	54	A6	41	AB	0F	2A	E4	86	0E	5C	C0	91	5B	EE	AA	92	T]A«.â†.\\À`[i*'
009C4150	8A	A1	3D	29	12	B8	0B	B3	1E	43	E0	6D	89	8D	75	98	Š;=).'.Câm.k.u"
009C4160	78	CF	2A	8A	02	D5	81	4D	BD	13	C8	E8	45	4E	70	A0	xI*Š.Ô.Mš.ÈèENp
009C4170	F9	A7	73	61	30	27	74	81	70	F4	18	12	75	05	CB	6B	ùŠsa0't.pò..u.Èk
009C4180	55	3A	24	4A	F7	68	06	B3	62	7E	E5	9F	13	2D	E3	EC	U:šJ-h.'b~âŸ.-âi
009C4190	79	64	BF	B5	35	6C	DA	F7	9E	89	36	EB	B5	DD	8C	38	ydçµ51Û+žñèµŸÈš
009C41A0	55	DC	09	AD	DD	FE	63	26	8F	CD	09	56	09	A8	16	8E	UÛ..Ÿpca.í.V..Ž
009C41B0	3A	CA	AF	3A	CA	54	FE	D1	49	67	42	98	59	8C	87	52	:È-ÈTpñIçB`Yç+R
009C41C0	94	C5	3D	5A	BC	36	B1	3C	72	02	80	23	D2	0B	59	2D	"À=246±<r.e#Ô.Y-
009C41D0	D3	1D	14	31	E2	A6	F9	6C	D7	4E	A2	FC	70	34	DA	FC	Ó...;ùl×Noùp4ÛÛ
009C41E0	2F	52	82	8D	E4	F0	E4	4F	97	53	85	38	E9	9B	08	C4	/Râ=èšòO-S..šé).À
009C41F0	B3	23	8E	2C	A7	04	F9	8E	39	7C	A9	BF	22	6C	38	2D	*šž,š.ùž9 øç"l8-
009C4200	00	40	9C	00	00	00	00	00	0A	00	00	00	00	00	00	00	.0æ.....

Figure 46

Indicators of Compromise

SHA256

f484f919ba6e36ff33e4fb391b8859a94d89c172a465964f99d6113b55ced429

Royal Ransom Note

README.txt

Process spawned

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