

A night cityscape with a digital globe overlay. The globe is composed of a network of blue lines and dots, representing a digital or data network. The city lights are reflected in the water in the foreground.

A Detailed Analysis of The Last Version of Conti Ransomware

Prepared by: LIFARS, LLC
Date: 10/08/2021

EXECUTIVE SUMMARY

Conti ransomware has been sold as a RaaS (Ransomware as a Service) in underground forums and it's usually deployed by other malware such as TrickBot and BazaLoader/BazarLoader. It can run with one of the following parameters: "-p", "-m", "-size", "-log" and "-nomutex". A new mutex called "YUIOGHJKCVBNMFGHJKTYQUWIETASKDHGZBDGSKL237782321344" can be created to ensure that only one instance of ransomware is running at a single time. The malware has the ability to only encrypt network shares ("-m net" parameter), local drives ("-m local" parameter), or both of them ("-m all" parameter). The volume shadow copies are deleted using wmic and COM objects. The algorithm used to encrypt files is ChaCha8, with the key and nonce being encrypted using an RSA public key.

ANALYSIS AND FINDINGS

SHA256: 4bfd58d4e4a6fe5e91b408bc190a24d352124902085f9c2da948ad7d79b72618

The malware obfuscates the stack strings and implements multiple custom algorithms to decrypt them. An example of a decryption algorithm is shown below, along with the decrypted string:

```

.text:00A62B65 mov     [ebp+var_25], 21h ; '!'
.text:00A62B69 mov     [ebp+var_24], 8
.text:00A62B6D mov     [ebp+var_23], 54h ; 'T'
.text:00A62B71 mov     [ebp+var_22], 8
.text:00A62B75 mov     [ebp+var_21], 27h ; '''
.text:00A62B79 mov     [ebp+var_20], 8
.text:00A62B7D mov     [ebp+var_1F], 21h ; '!'
.text:00A62B81 mov     [ebp+var_1E], 8
.text:00A62B85 mov     [ebp+var_1D], 50h ; 'P'
.text:00A62B89 mov     [ebp+var_1C], 8
.text:00A62B8D mov     [ebp+var_1B], 2Ah ; '*'
.text:00A62B91 mov     [ebp+var_1A], 8
.text:00A62B95 mov     [ebp+var_19], 7Eh ; '~'
.text:00A62B99 mov     [ebp+var_18], 8
.text:00A62B9D mov     [ebp+var_17], 51h ; 'Q'
.text:00A62BA1 mov     [ebp+var_16], 8
.text:00A62BA5 mov     [ebp+var_15], 75h ; 'u'
.text:00A62BA9 mov     [ebp+var_14], 8
.text:00A62BAD mov     [ebp+var_13], 50h ; 'P'
.text:00A62BB1 mov     [ebp+var_12], 8
.text:00A62BB5 mov     [ebp+var_11], 50h ; 'P'
.text:00A62BB9 mov     [ebp+var_10], 8
.text:00A62BD0 mov     [ebp+var_9], 8
.text:00A62BC1 mov     a1, [ebp+var_27]
.text:00A62BC5 mov     [ebp+var_28], 0
.text:00A62BC8 cmp     [ebp+var_28], 0
.text:00A62BCC jnz     short loc_A62BFD
    
```

```

.text:00A62BCE xor     esi, esi
.text:00A62BD0 lea     edi, [esi+7Fh]
    
```

```

.text:00A62BD3 loc_A62BD3:
.text:00A62BD3 mov     al, [ebp+esi+var_27]
.text:00A62BD7 mov     ecx, 8
.text:00A62BDC movzx   eax, al
.text:00A62BDF sub     ecx, eax
.text:00A62BE1 mov     eax, ecx
.text:00A62BE3 shl     eax, 5
.text:00A62BE6 sub     eax, ecx
.text:00A62BE8 add     eax, eax
.text:00A62BEA cdq
.text:00A62BEB idiv   edi
.text:00A62BED lea     eax, [edx+7Fh]
.text:00A62BF0 cdq
.text:00A62BF1 idiv   edi
.text:00A62BF3 mov     [ebp+esi+var_27], dl
.text:00A62BF7 inc     esi
.text:00A62BF8 cmp     esi, 1Ah
.text:00A62BF8 jnb     short loc_A62BD3
    
```

Figure 1

Address	Hex	ASCII
00B9FE29	4B 00 65 00 72 00 6E 00 65 00 6C 00 33 00 32 00	K.e.r.n.e.l.3.2.
00B9FE39	2E 00 64 00 6C 00 6C 00 00 00 02 28 4C C3 02 02	..d.l.l... (LA..

Figure 2

The relevant APIs are imported dynamically at runtime using some hashing algorithms (the first parameter is a hash value; the second parameter is an offset). The return value is placed into the EAX register:

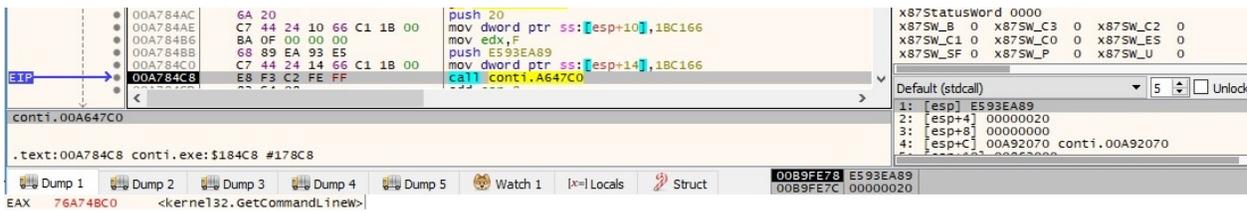


Figure 3

The binary retrieves the command-line string for the process by calling the GetCommandLineW API:



Figure 4

CommandLineToArgvW is utilized to extract an array of pointers to the command line arguments, as shown in figure 5:

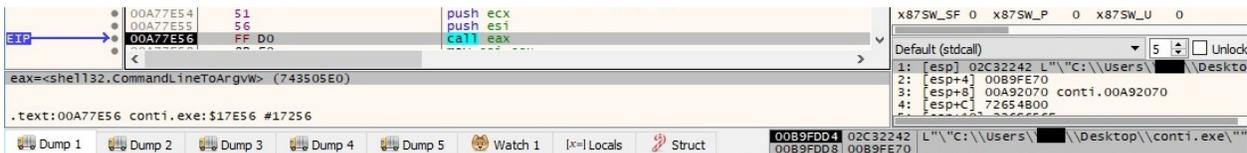


Figure 5

The following strings have been decrypted using algorithms like the one presented in figure 1:

Address	Hex	ASCII
00B9FE69	2D 00 70 00 00 00 00 01 00 00 00 7E EB A8 90 04	-.p.....~è..
Address	Hex	ASCII
00B9FE61	2D 00 6D 00 00 00 00 00 2D 00 70 00 00 00 00 01	-.m.....-p.....
Address	Hex	ASCII
00B9FE3D	2D 00 6C 00 6F 00 67 00 00 00 76 C0 4B A7 76 56	-.l.o.g...vAK\$vv
Address	Hex	ASCII
00B9FE2D	2D 00 73 00 69 00 7A 00 65 00 00 00 32 2E 64 00	-.s.i.z.e...2.d.
Address	Hex	ASCII
00B9FDF5	2D 00 6E 00 6F 00 6D 00 75 00 74 00 65 00 78 00	-.n.o.m.u.t.e.x.
Address	Hex	ASCII
00B9FE91	59 55 49 4F 47 48 4A 4B 43 56 56 42 4E 4D 46 47	YUIOGHJKCVBNMFG
00B9FEA1	48 4A 4B 54 59 51 55 57 49 45 54 41 53 4B 44 48	HJKTYQUWIETASKDH
00B9FEB1	47 5A 42 44 47 53 4B 4C 32 33 37 37 38 32 33 32	GZBDGSKL23778232
00B9FEC1	31 33 34 34 00 86 00 00 00 00 00 C8 FE B9 00 00	1344.....Eb'..
Address	Hex	ASCII
00B9FC2D	65 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00	E.x.p.l.o.r.e.r.
00B9FC3D	2E 00 65 00 78 00 65 00 00 00 00 2C 02 00 00 00	..e.x.e.....
Address	Hex	ASCII
00B9F5A9	5F 00 5F 00 50 00 72 00 6F 00 76 00 69 00 64 00	..P.r.o.v.i.d.
00B9F5B9	65 00 72 00 41 00 72 00 63 00 68 00 69 00 74 00	e.r.A.r.c.h.i.t.
00B9F5C9	65 00 63 00 74 00 75 00 72 00 65 00 00 00 00 F8	e.c.t.u.r.e....o
Address	Hex	ASCII
00B9F5D9	52 00 4F 00 4F 00 54 00 5C 00 43 00 49 00 4D 00	R.O.O.T.\.C.I.M.
00B9F5E9	56 00 32 00 00 00 02 FC FF FF FF A0 07 00 00 58	V.2....üvyv...X
Address	Hex	ASCII
00B9F5F1	57 00 51 00 4C 00 00 00 17 7D 00 00 60 86 00 00	W.Q.L....}..
Address	Hex	ASCII
00B9F569	53 00 45 00 4C 00 45 00 43 00 54 00 20 00 2A 00	S.E.L.E.C.T. *.
00B9F579	20 00 46 00 52 00 4F 00 4D 00 20 00 57 00 69 00	.F.R.O.M. W.i.
00B9F589	6E 00 33 00 32 00 5F 00 53 00 68 00 61 00 64 00	n.3.2..S.h.a.d.
00B9F599	6F 00 77 00 43 00 6F 00 70 00 79 00 00 00 00 00	o.w.C.o.p.y.....
Address	Hex	ASCII
00B9F89D	46 00 6F 00 75 00 6E 00 64 00 20 00 25 00 64 00	F.o.u.n.d. %.d.
00B9F8AD	20 00 64 00 72 00 69 00 76 00 65 00 73 00 3A 00	.d.r.i.v.e.s.:.
Address	Hex	ASCII
00B9F5C5	31 37 32 2E 00 00 00 00 4F 6C 65 EC F1 04 77 EC	172.....0leñ.wi
Address	Hex	ASCII
00B9F5B1	31 39 32 2E 31 36 38 2E 00 32 2E 64 6C 6C 00 00	192.168..2.d11..
Address	Hex	ASCII
00B9F5CD	31 30 2E 00 F1 04 77 EC 01 00 00 FC F5 B9 00 C0	10..ñ.wi...üö'.A
Address	Hex	ASCII
00B9F5BD	31 36 39 2E 00 74 64 00 31 37 32 2E 00 00 00 00	169..td.172.....

Figure 6

The executable creates a mutex called "YUIOGHJKCVBNMFGHJKTYQUWIETASKDHGZBDGSKL237782321344" (if the malware runs with the "-nomutex" parameter, then no mutex is created):

The screenshot shows a debugger window with assembly code at address 00A78647: `push ecx`, `push 1`, `push 0`, and `call eax`. The 'eax' register contains the address of `kernel32.CreateMutexA`. The stack dump shows the arguments: `cont1.exe:18647 #17A47`, `cont1.00A92070`, and the mutex name `YUIOGHJKCVBNMFGHJKTYQUWIETASKDHGZBDGSKL237782321344`.

Figure 7

GetNativeSystemInfo is used to retrieve information about the system:

The screenshot shows a debugger window with assembly code at address 00A786E7: `push ecx` and `call eax`. The 'eax' register contains the address of `kernel32.GetNativeSystemInfo`. The stack dump shows the arguments: `cont1.exe:186E7 #17AE7`, `cont1.00A92070`, and the system information structure `&L"winsta0\Default"`.

Figure 8

The malicious file creates 2 (which is the number of processors) threads that will handle the files encryption, as we'll describe in the upcoming paragraphs:

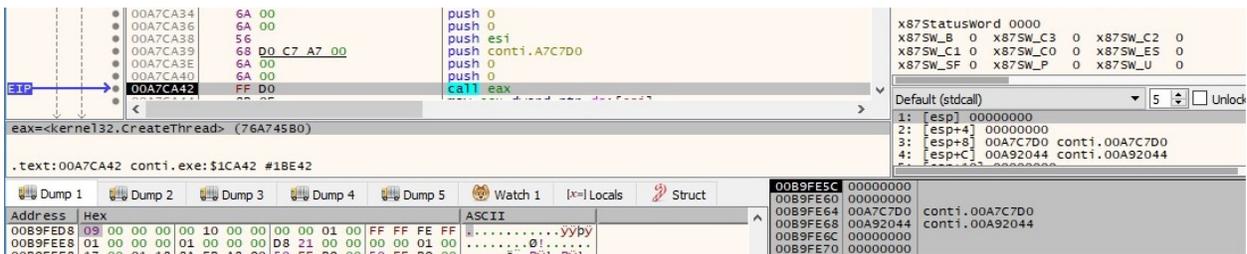


Figure 9

The executable takes a snapshot of all processes in the system by calling the CreateToolhelp32Snapshot routine (0x2 = **TH32CS_SNAPPROCESS**):



Figure 10

The processes are enumerated using the Process32FirstW and Process32NextW APIs:

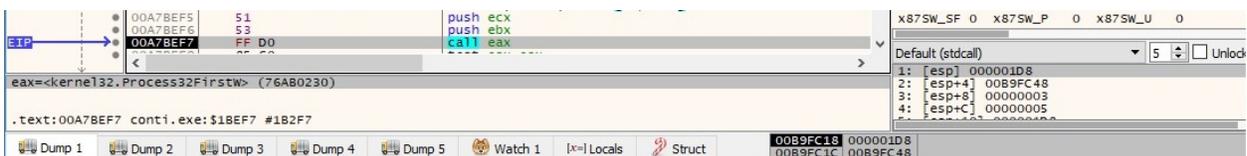


Figure 11

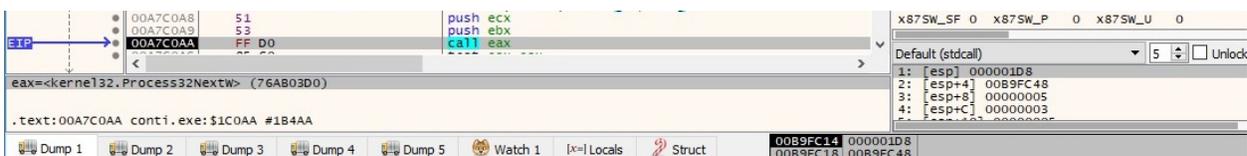


Figure 12

The malware searches for the "explorer.exe" process and saves its ID into a buffer for later use. The CoInitializeEx function is utilized to initialize the COM library for use by the thread, as highlighted below:



Figure 13

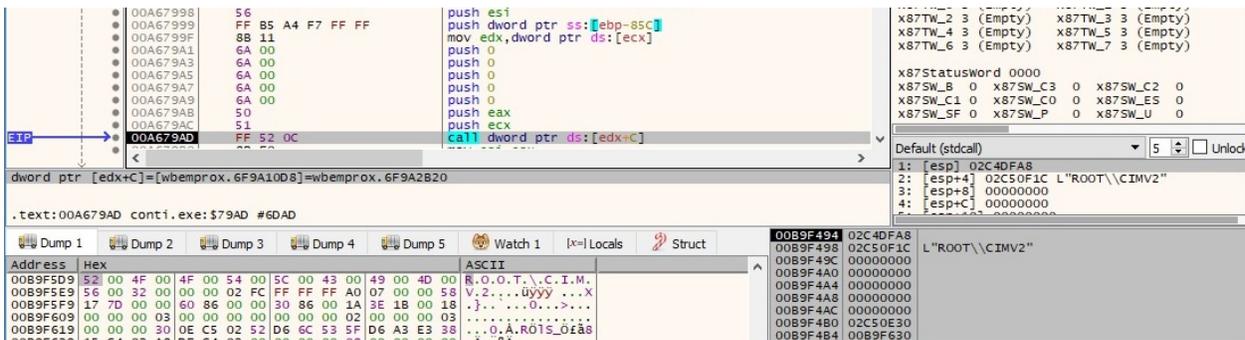


Figure 17

The binary sets the authentication information that is used to make calls on a proxy via a CoSetProxyBlanket API call (0xA = **RPC_C_AUTHN_WINNT**, 0x3 = **RPC_C_AUTHN_LEVEL_CALL**, 0x3 = **RPC_C_IMP_LEVEL_IMPERSONATE**):

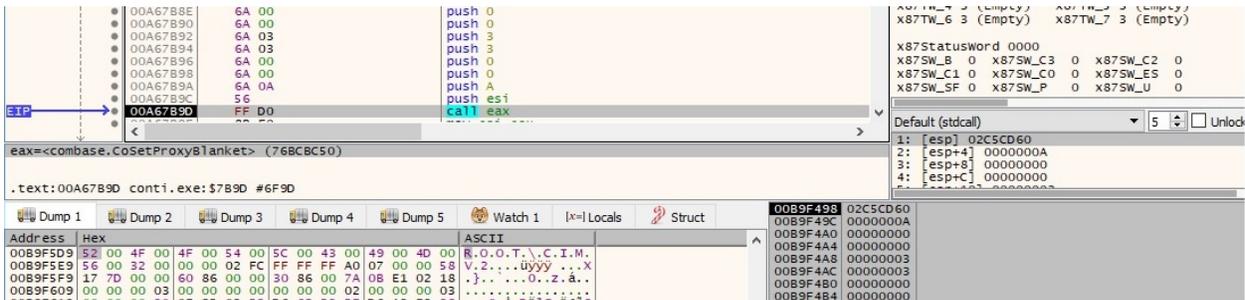


Figure 18

The following WQL (SQL for WMI) query is executed by the ransomware:

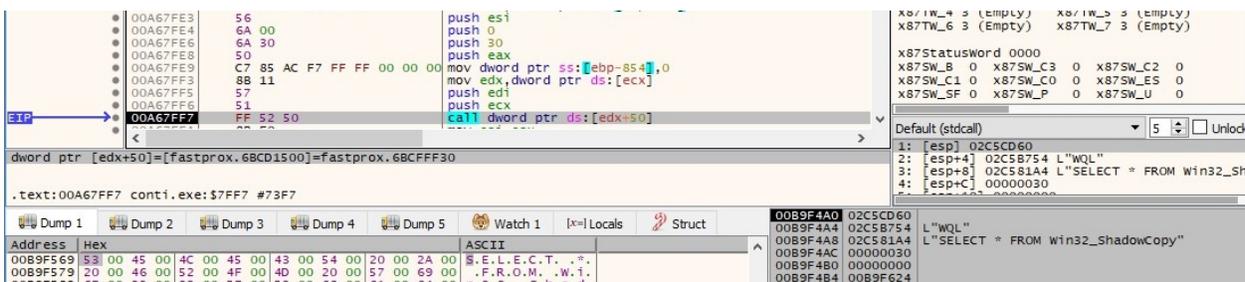


Figure 19

For each volume shadow copy, the binary extracts its ID using the Get method:



Figure 24

The valid drives on the system are retrieved by calling the GetLogicalDriveStringsW function:

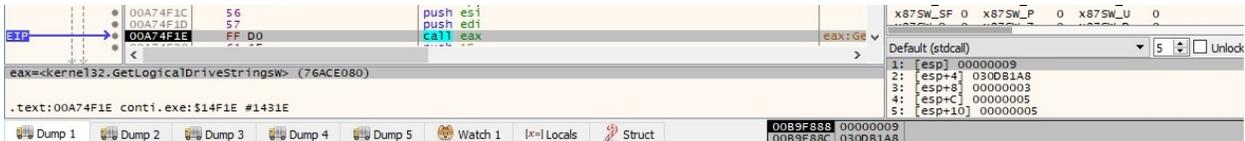


Figure 25

There is a function call to WSASStartup that initiates the use of the Winsock DLL:



Figure 26

A new socket is created by the process (0x2 = **AF_INET**, 0x1 = **SOCK_STREAM**, 0x6 = **IPPROTO_TCP**):

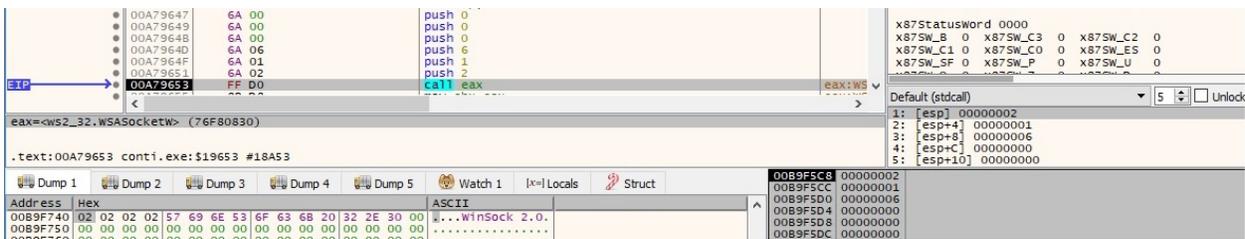


Figure 27

The malicious process calls the WSAIocctl function with the **SIO_GET_EXTENSION_FUNCTION_POINTER** command code in order to invoke an extension function, as shown in figure 28:

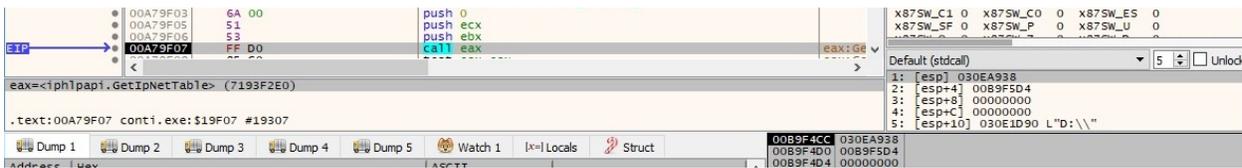


Figure 32

Each IP address extracted above is converted into a string (dotted-decimal format):

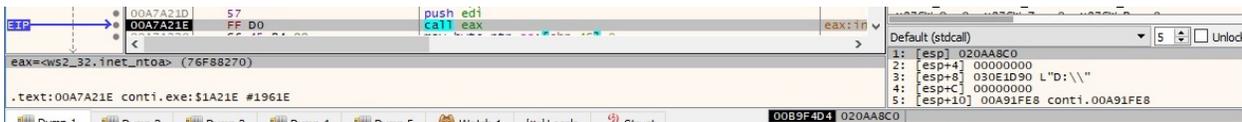


Figure 33

The malware is only interested in local IP addresses because it compares every IP address with the prefixes "172.", "192.168.", "10." and "169.". The binary creates 2 new threads via a function call to CreateThread:

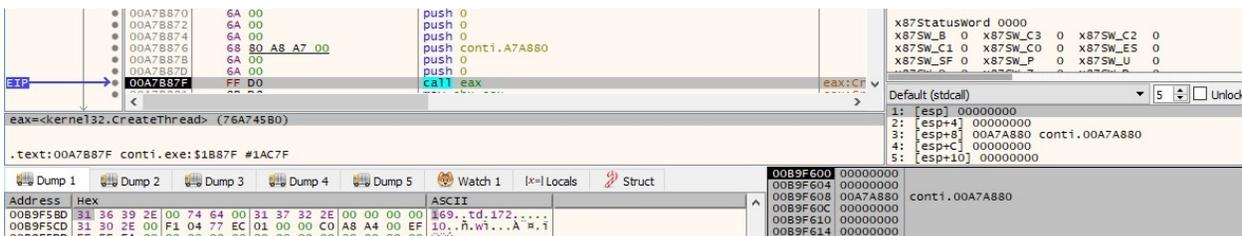


Figure 34

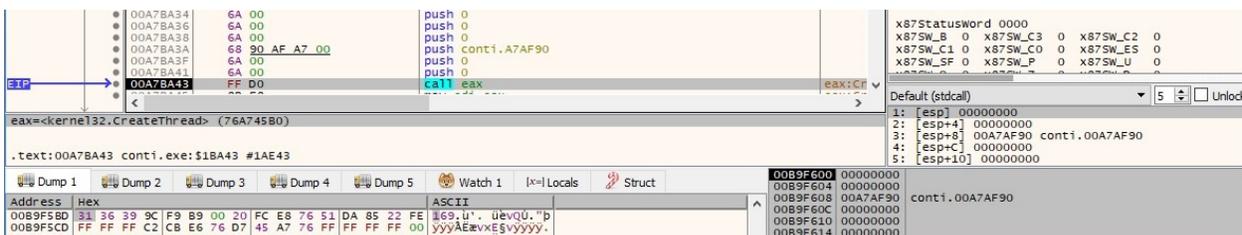


Figure 35

PostQueuedCompletionStatus is utilized to send an I/O completion packet to the completion port created earlier (**dwCompletionKey** = 0x1):

Figure 36

THREAD ACTIVITY – SUB_A7AF90 FUNCTION

The file creates a queue for timers (which are objects that allow the user to specify a function that will be called at a particular time):

Figure 37

The ransomware attempts to extract the I/O completion packet from the I/O completion port (sent by the main thread) by calling the GetQueuedCompletionStatus routine:

Figure 38

A new socket is created by calling the WSASocketW API (0x2 = **AF_INET**, 0x1 = **SOCK_STREAM**, 0x6 = **IPPROTO_TCP**, 0x1 = **WSA_FLAG_OVERLAPPED**):

Figure 39

The bind routine associates the local address with the above socket:

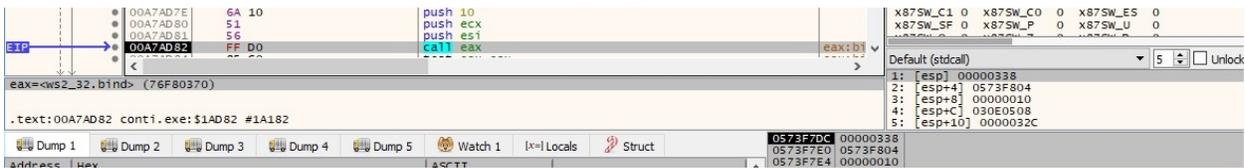


Figure 40

CreateIoCompletionPort is utilized to associate the socket created above with the I/O completion port. After this operation is complete, the process can receive notifications of the completion of I/O operations involving the socket handle (**CompletionKey** = 0x2):

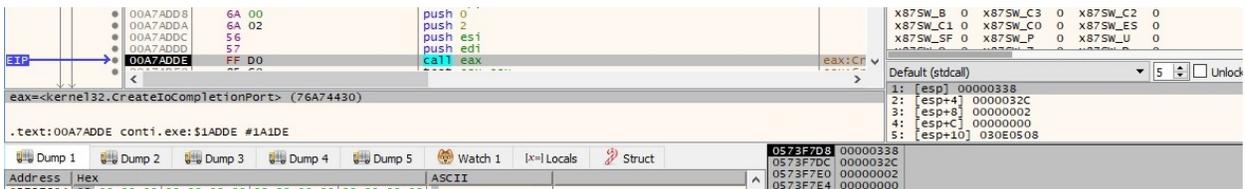


Figure 41

The binary converts a port number (445) from network byte order to host byte order:

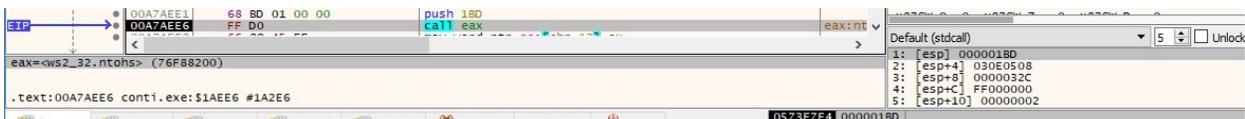


Figure 42

The malware tries to connect to different IP addresses on port 445 (192.168.10.x and 192.168.164.x) using the LPFN_CONNECTEX function, as described below:

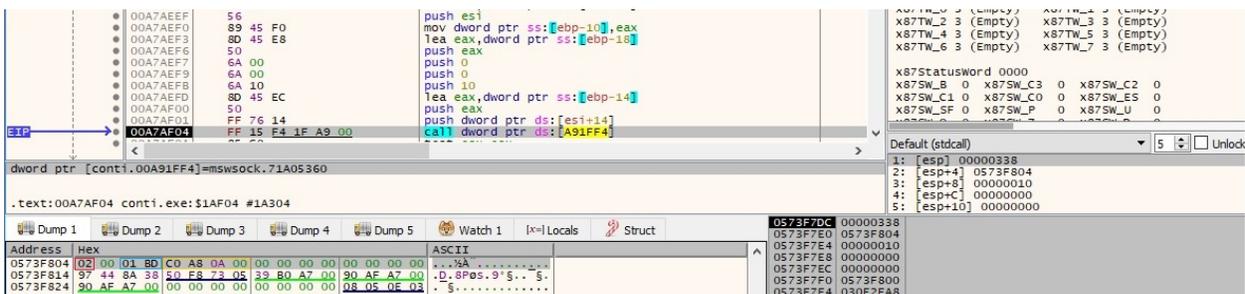


Figure 43

The CreateTimerQueueTimer routine is used to create a timer-queue timer, which expires at a specific time (0x7530 = 30000ms = 30 seconds) and then a callback function is called:

```

00A7B28D 6A 00          push 0
00A7B291 68 30 75 00 00 push 7530
00A7B296 6A 00          push 0
00A7B298 68 50 AF A7 00 push cont1.A7AF60
00A7B29D 57           push esi
00A7B29E 51           push ecx
00A7B29F FF D0       call eax

```

eax=<kernel32.CreateTimerQueueTimer> (76A745F0)

.text:00A7B29F cont1.exe:\$1B29F #1A69F

Address	Hex	ASCII
0573F804	38 F8 73 05 08 05 0F 03	80s.....\$....
0573F814	30 75 00 00 00 00 00 00	00.....00.....
0573F824	20 AF A7 00 00 00 00 00	00.....08 05 0E 03

Figure 44

The setsockopt API is utilized to set the **SO_UPDATE_CONNECT_CONTEXT** option, which updates the properties of the socket after a connection is established (0xFFFF = **SOL_SOCKET**, 0x7010 = **SO_UPDATE_CONNECT_CONTEXT**):

```

00A7B07F 6A 00          push 0
00A7B081 6A 00          push 0
00A7B083 68 10 70 00 00 push 7010
00A7B088 68 FF FF 00 00 push FFFF
00A7B08D 56           push esi
00A7B08E FF D0       call eax

```

eax=<ws2_32.setsockopt> (76F7F880)

.text:00A7B08E cont1.exe:\$1A48E

Address	Hex	ASCII
0573F804	00 00 00 00 B8 01 00 008...YY..
0573F814	38 03 00 00 FF FF 00 008...YY..

Figure 45

The file retrieves the **SO_CONNECT_TIME** option, which represents the number of seconds a socket was connected (0xFFFF = **SOL_SOCKET**, 0x700C = **SO_CONNECT_TIME**):

```

00A7B0B2 51           push ecx
00A7B0B3 8D 4C 24 28 lea ecx,dword ptr ss:[esp+28]
00A7B0B7 51           push ecx
00A7B0B8 68 0C 70 00 00 push 700C
00A7B0BD 68 FF FF 00 00 push FFFF
00A7B0C2 56           push esi
00A7B0C3 FF D0       call eax

```

eax=<ws2_32.getsockopt> (76F86E70)

.text:00A7B0C3 cont1.exe:\$1A4C3

Address	Hex	ASCII
0573F804	00 00 00 00 FC 00 00 00U...YY..
0573F814	38 03 00 00 FF FF 00 008...YY..

Figure 46

Whether the sample has successfully established a connection to a particular IP address, then it calls the WSAddressToStringW routine to convert the components of that sockaddr structure into a human-readable string:

```

00A7ABF9 51           push ecx
00A7ABFA lea ecx,dword ptr ds:[esi+4]
00A7ABFD 51           push ecx
00A7ABFE 6A 00          push 0
00A7AC00 6A 10          push 10
00A7AC02 lea ecx,dword ptr ss:[ebp-18]
00A7AC05 56           push esi
00A7AC06 FF D0       call eax

```

eax=<ws2_32.WSAddressToStringW> (76F841C0)

.text:00A7AC06 cont1.exe:\$1A006

Address	Hex	ASCII
0573F800	02 00 00 00 C0 A8 0A 00	...A.A.S...
0573F810	02 00 00 00 C5 B0 A7 00	...A.A.S...

Figure 47

PostQueuedCompletionStatus is utilized to send an I/O completion packet to the completion port created before (**dwCompletionKey = 0x3**):

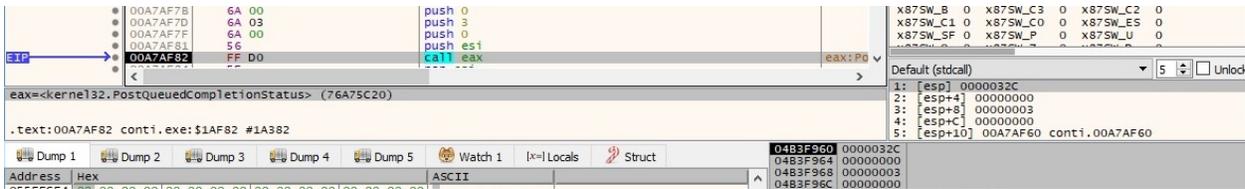


Figure 48

The binary shuts down send operations for the socket (0x1 = **SD_SEND**):



Figure 49

THREAD ACTIVITY – SUB_A7A880 FUNCTION

The NetShareEnum function is utilized to retrieve information about the network shares available on other computers:

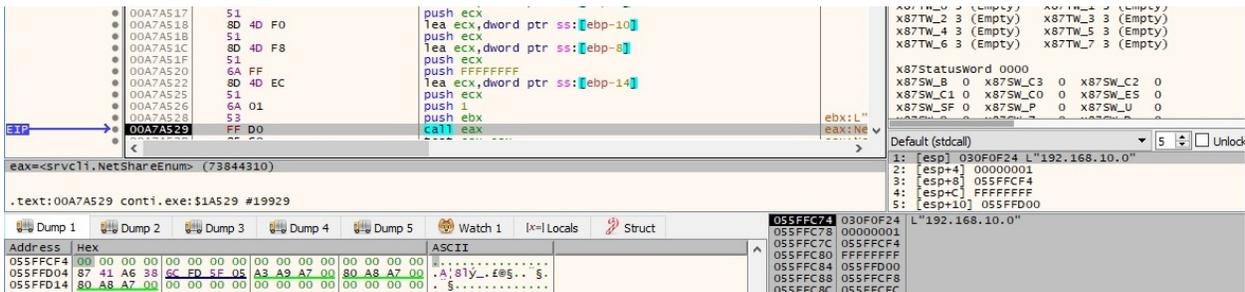


Figure 50

Some strings that will be written in the log file (if logging mode is enabled) are also decrypted using custom algorithms:

Address	Hex	ASCII
055FFCD5	41 00 44 00 4D 00 49 00 4E 00 24 00 00 00 05 CC	A.D.M.I.N.\$...I
055FFCAD	46 00 6F 00 75 00 6E 00 64 00 20 00 73 00 68 00	F.o.u.n.d. .s.h.
055FFCBD	61 00 72 00 65 00 20 00 25 00 73 00 2E 00 00 00	a.r.e. .%.s.....
055FFD21	53 00 74 00 61 00 72 00 74 00 69 00 6E 00 67 00	S.t.a.r.t.i.n.g.
055FFD31	20 00 73 00 65 00 61 00 72 00 63 00 68 00 20 00	.s.e.a.r.c.h..
055FFD41	6F 00 6E 00 20 00 73 00 68 00 61 00 72 00 65 00	o.n. .s.h.a.r.e..
055FFD51	20 00 25 00 73 00 2E 00 00 00 00 00 54 11 03 40	%.s.....T.?

Figure 51

The "ADMIN\$" share will not be targeted by the malware (the others will be encrypted):

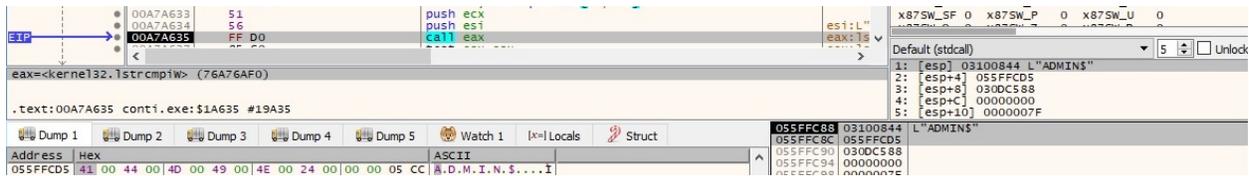


Figure 52

THREAD ACTIVITY – SUB_A7C7D0 FUNCTION

CryptAcquireContextA is used to obtain a handle to a key container within a CSP (0x18 = PROV_RSA_AES, 0xF0000000 = CRYPT_VERIFYCONTEXT):

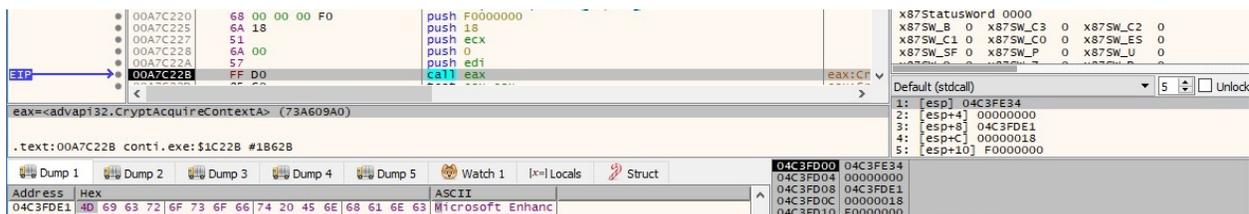


Figure 53

An RSA public key is imported via a CryptImportKey function call:

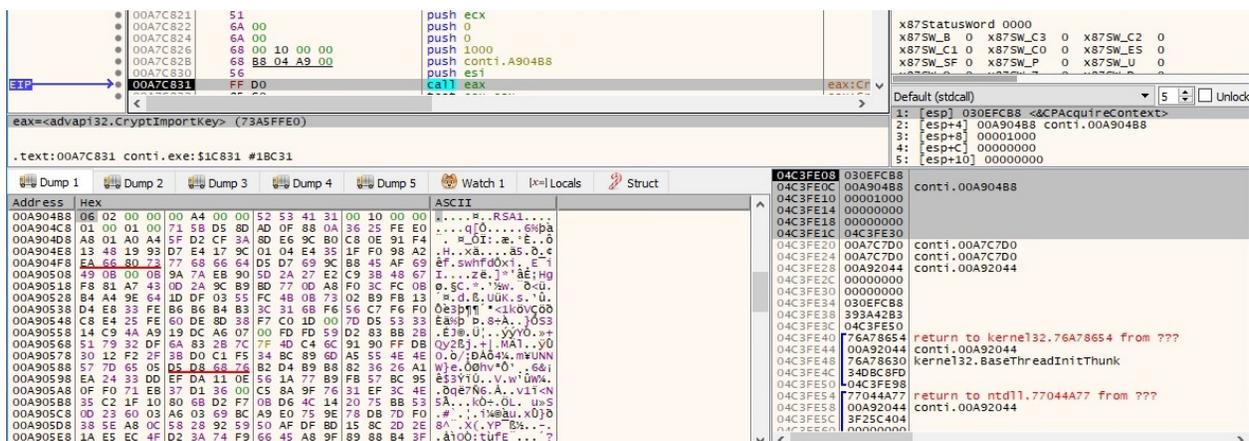


Figure 54

The process creates a file called "readme.txt" in every folder that it encrypts (0x40000000 = GENERIC_WRITE, 0x2 = CREATE_ALWAYS):

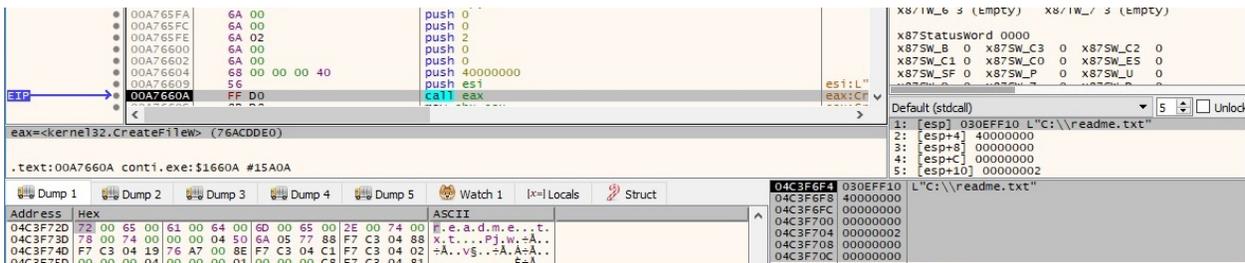


Figure 55

The following 4-byte values suggest that the encryption algorithm is a ChaCha cipher (Ref. <https://arxiv.org/pdf/1907.11941.pdf>):

```
.text:00A766EA push esi
.text:00A766EB push edi
.text:00A766EC mov [ebp+var_80], 61707865h
.text:00A766F3 mov [ebp+var_7C], 3320646Eh
.text:00A766FA mov [ebp+var_78], 79622D32h
.text:00A76701 mov [ebp+var_74], 6B206574h
.text:00A76708 mov [ebp+var_44], eax
.text:00A7670B call sub_A65AF0
```

Figure 56

The encrypted content of the ransom note is decrypted using the ChaCha algorithm, and the file is populated by calling the WriteFile routine, as highlighted in figure 57.

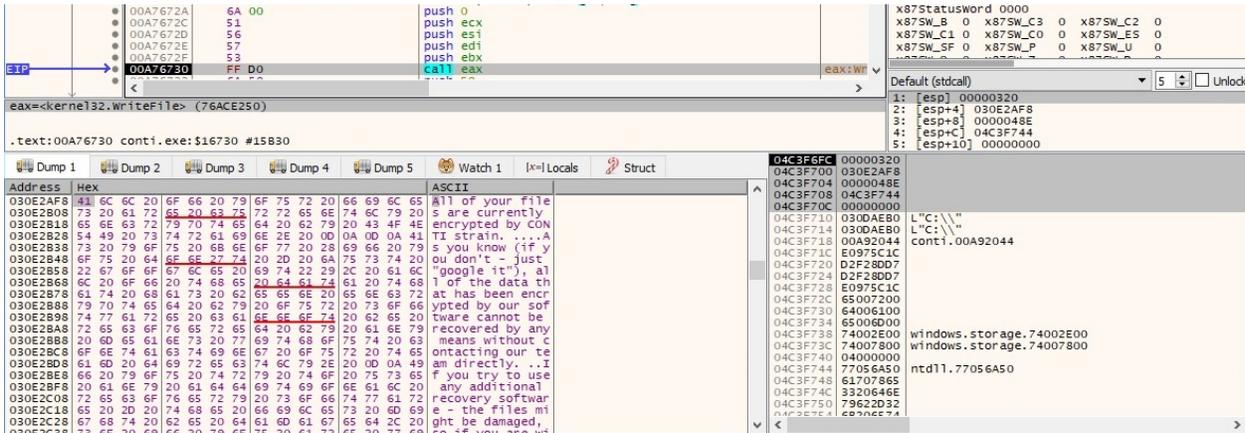


Figure 57

The files are enumerated in the targeted directory using the FindFirstFileW and FindNextFileW APIs:

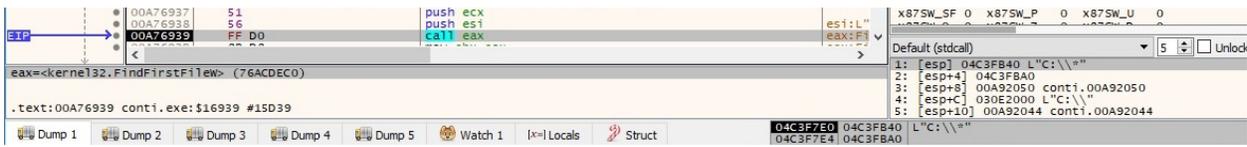


Figure 58

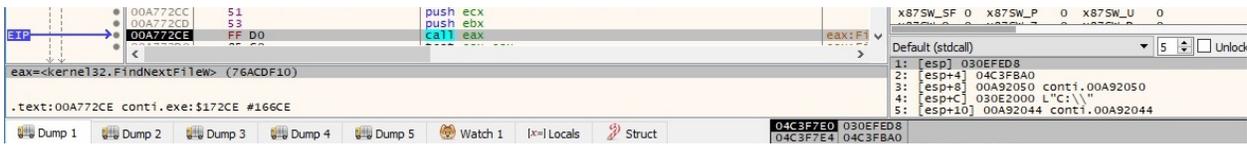


Figure 59

There is a comparison between the directory name and a list of directories that will be skipped by the ransomware:

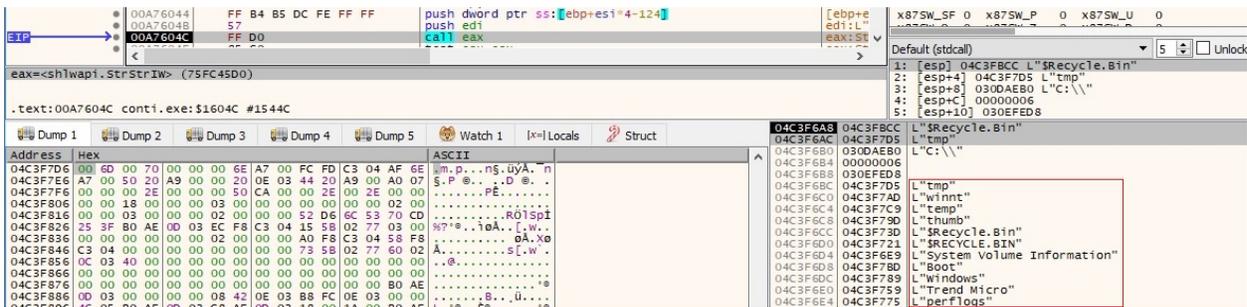


Figure 60

The PathIsDirectoryW routine is utilized to determine whether a path is a valid directory:

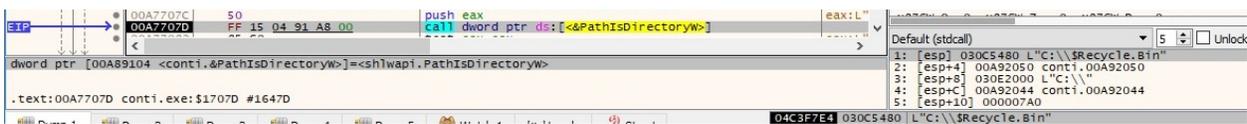


Figure 61

The following files/files extensions will also be skipped by Conti:

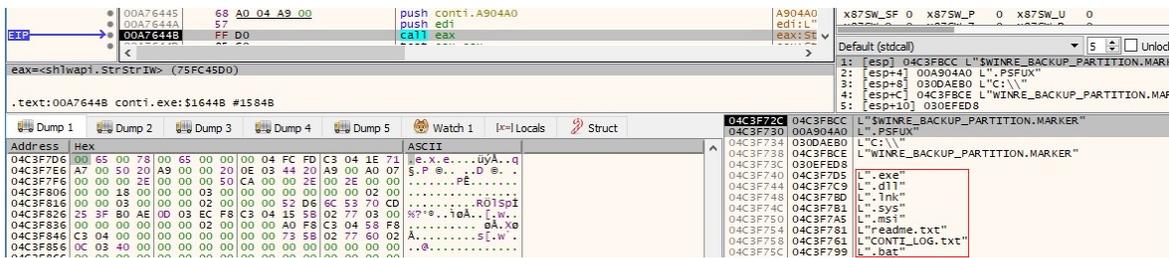


Figure 62

The sample descrypts the following DLL names: OleAut32.dll, Rstrtmgr.dll, Iphlpapi.dll, Netapi32.dll, Advapi32.dll, Kernel32.dll, Shell32.dll, Shlwapi.dll, ws2_32.dll, User32.dll, ntdll.dll, Ole32.dll. The GetModuleHandleA function is utilized to retrieve a handle for these DLLs. The malware generates 32 random bytes by calling the CryptGenRandom routine (this will be used as the ChaCha key):

Figure 63

There is also a call to CryptGenRandom that generates 8 random bytes, which will be used as the ChaCha8 nonce (this is the moment when we can tell for sure that the encryption algorithm for files is ChaCha8):

Figure 64

The ChaCha8 key and nonce are encrypted using the RSA public key:

Figure 65

The ransomware retrieves file system attributes for the targeted file:

Figure 66

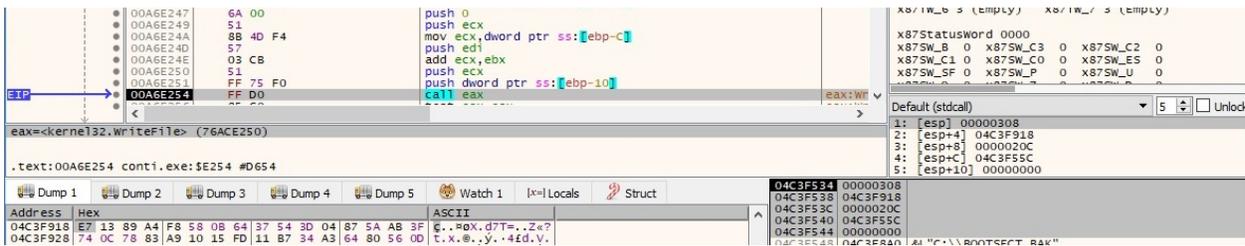


Figure 70

There are 3 different cases depending on the file size: small files (< 1MB), medium files (between 1MB and 5MB), and large files (> 5MB). In the case of medium and large files, there exist 2 sub-cases depending on the file extension (if it belongs to the targeted lists or not). The following 10-byte buffer that contains a marker (0x24) and the file size (0x2000) is appended to the encrypted file:

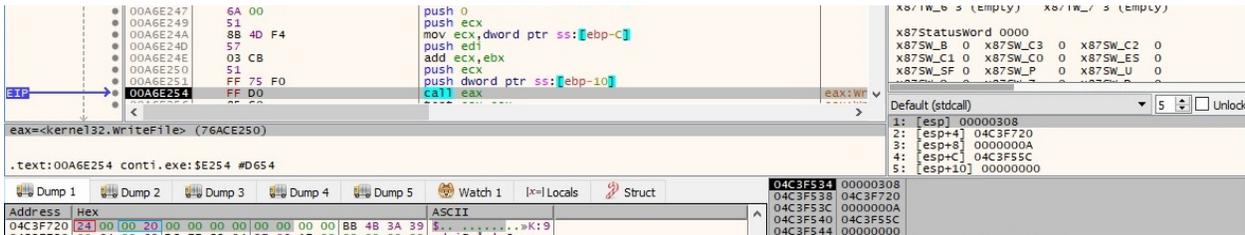


Figure 71

The binary reads the file content using the ReadFile function:

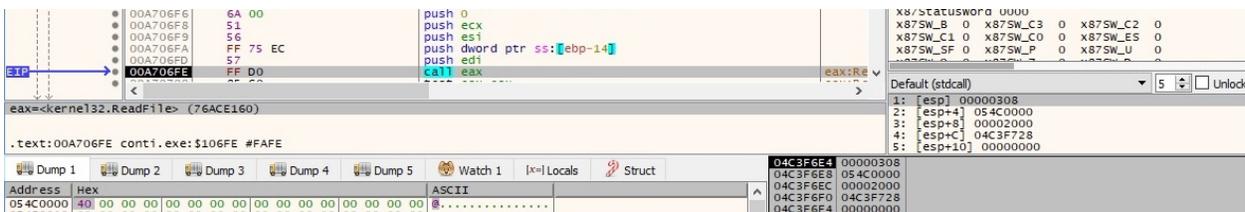


Figure 72

Address	Hex	ASCII
054C0000	EB 52 90 4E 54 46 53 20 20 20 00 02 08 00 00	ER.NTFS
054C0010	00 00 00 00 00 F8 00 00 3F 00 FF 00 00 08 00 000..?..y.....
054C0020	00 00 00 00 80 00 80 00 6D 4A F1 09 00 00 00 00mJh.....
054C0030	00 00 0C 00 00 00 00 00 02 00 00 00 00 00 00
054C0040	F6 00 00 00 01 00 00 00 2F AD C9 A2 BC C9 A2 4A/..Ee%eCj
054C0050	00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07ú3A.D% úhA
054C0060	1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E	..hf.E.....f.>..N
054C0070	54 46 53 75 15 84 41 8B AA 55 CD 13 72 0C 81 FB	TFSu..A%úI..r..ú
054C0080	55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC	U%u..A..u.eý..ú
054C0090	18 68 1A 00 84 48 8A 16 0E 00 8B F4 16 1F CD 13	..h..H.....ö..I.
054C00A0	9F 83 C4 18 9E 58 1F 72 E1 3B 06 08 00 75 DB A3	..A..X..rã;...u0g
054C00B0	0F 00 C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8	fy.....z3D'..e
054C00C0	66 FF 06 11 00 03 16 0F 00 8E C2 FF 06 16 00 E8	K..eWt'..I..f#Au
054C00D0	48 00 28 C8 77 EF B8 00 00 BB CD 1A 66 23 C0 75 2D	h..úTCPAú..r..
054C00E0	66 81 F8 54 43 50 41 75 24 81 F9 02 01 72 1E 1F	h..hR..h..fSfSf
054C00F0	68 07 B8 16 68 52 11 16 68 09 00 66 53 66 53 66	U..h..fa..i.3Aú
054C0100	55 16 16 16 68 B8 01 66 61 0E 07 CD 1A 33 C0 BF	..ö..úö*ép..f..
054C0110	0A 13 B9 F6 0C FC F3 AA E9 FE 01 90 90 66 60 1E	..fi..f.....fh...
054C0120	06 66 A1 11 00 66 03 06 1C 00 1E 66 68 00 00 00	..fp.Sh..h..B...
054C0130	00 66 50 06 53 68 01 00 68 10 00 B4 42 8A 16 0E	..Ät..v[7fxfv]
054C0140	00 16 15 8E 54 CD 12 66 58 58 FA 66 58 66 58 1E	

Figure 73

The content is encrypted using the ChaCha8 algorithm implemented by Conti:

Address	Hex	ASCII
054C0000	5C 12 56 1C C7 23 B7 0A 56 5C 66 53 C7 06 D6 E1	N.V.Ç#.V\fsç.Ôâ
054C0010	5E 0D CD 90 B4 38 89 68 04 F5 D0 20 B6 48 B5 A3	^,I.;.h.ÖD ¶Huf
054C0020	F2 65 1E 51 1C 8E 93 55 32 24 A9 07 B5 25 2D 83	öe.Q...U2\$@.µ%-.
054C0030	1E B8 16 18 74 13 F6 15 87 38 32 75 8D B2 72 57	...t.ö.;2u.*rW
054C0040	C4 7D 93 5C 44 0C FA C3 00 51 E2 09 83 F8 58 CC	Äj.\D.úA.Qâ..øXI
054C0050	1E 55 9C 69 8E 83 10 CE CA 24 D0 A5 BF C8 13 84	.U.î.*.îÊ\$Ð#¿Ë..
054C0060	B1 4E 37 B7 38 80 D5 5E 6D B5 98 A5 7A F3 A0 75	±N7.8°0^µj.¿z0 u
054C0070	55 47 EB 77 13 69 98 59 66 0C 7E 19 E0 82 11 22	UGëw.i.Yf.~,a.."
054C0080	69 EA 5A 47 AD 9E D4 A5 25 DB 75 F3 97 55 52 62	îÊZG.0¿%0uó.URb
054C0090	EE A4 86 B5 76 02 2E AA A0 8E 18 20 E5 E9 70 D2	îr.µv..*. äép0
054C00A0	C4 00 A9 06 71 EA 47 86 04 B9 12 5F C7 FA D7 F7	A.@.qëG...Cúx±
054C00B0	B7 11 08 33 CE 88 04 7F C6 55 D1 D2 52 A6 F2 08	..3î...EUNOR'b.
054C00C0	BF 05 F9 7D EC 2E 3E 76 CA A8 9A 4A 55 65 A7 D5	¿.ú}ü.>vÉ..JUeş0
054C00D0	1D 40 5F 98 91 47 E1 D4 6A DA 07 06 59 BE FA 11	@_..Gã0jÜ..%µ
054C00E0	EB 62 EB 6A 4F 37 70 59 F0 A8 D2 27 45 F9 5C E2	êbëj07py0'0'Eu\â
054C00F0	C6 3D FA 70 C7 7C 54 87 64 07 1F D2 8F D5 1A 2D	Æ=úpÇ T.d..0.0.-
054C0100	96 34 B2 7A 58 54 DB 37 B0 00 5F 28 07 A7 1F 8B	.4*¿[T07°_..(,ç.»
054C0110	92 85 73 E3 77 BC D2 40 7D 14 7D 82 ED 36 92 52	..sãw40ë}.j.16.R
054C0120	F6 42 E0 DE 22 D3 70 B9 A1 A1 41 0B C8 54 09 B9	0Bâb'0p'ijA.ÊT.0
054C0130	33 46 20 36 40 58 D9 A3 44 37 3B 54 59 CC 1A 4F	3F 6@xUêD7;TYI.0
054C0140	00 7C 06 84 AF 7D 64 14 DF 48 08 41 9C FF C1 A4	l -¿d ðv. Åx. Åb

Figure 74

A snippet of the ChaCha8 algorithm developed by the ransomware is presented in figure 75.

```

.text:00A65C83
.text:00A65C83 loc_A65C83:
.text:00A65C83 add     edi, [ebp+var_60]
.text:00A65C86 mov     eax, [ebp+var_58]
.text:00A65C89 xor     ebx, edi
.text:00A65C8B add     ecx, [ebp+var_78]
.text:00A65C8E rol     ebx, 10h
.text:00A65C91 xor     edx, ecx
.text:00A65C93 add     eax, ebx
.text:00A65C95 mov     [ebp+var_5C], edi
.text:00A65C98 mov     [ebp+var_58], eax
.text:00A65C9B xor     eax, [ebp+var_60]
.text:00A65C9E rol     eax, 0Ch
.text:00A65CA1 add     edi, eax
.text:00A65CA3 rol     edx, 10h
.text:00A65CA6 xor     ebx, edi
.text:00A65CAB mov     [ebp+var_5C], edi
.text:00A65CAB mov     edi, [ebp+var_58]
.text:00A65CAE rol     ebx, 8
.text:00A65CB1 add     edi, ebx
.text:00A65CB3 mov     [ebp+var_58], edi
.text:00A65CB6 xor     edi, eax
.text:00A65CB8 mov     eax, [ebp+var_4C]
.text:00A65CBB add     eax, edx
.text:00A65CBD rol     edi, 7
.text:00A65CC0 mov     [ebp+var_4C], eax
.text:00A65CC3 xor     eax, [ebp+var_78]
.text:00A65CC6 rol     eax, 0Ch
.text:00A65CC9 add     ecx, eax
.text:00A65CCB xor     edx, ecx
.text:00A65CCD mov     [ebp+var_84], ecx
.text:00A65CD3 mov     ecx, [ebp+var_4C]
.text:00A65CD6 rol     edx, 8
.text:00A65CD9 add     ecx, edx
.text:00A65CDB mov     [ebp+var_60], edx
.text:00A65CDE mov     edx, [ebp+var_64]
.text:00A65CE1 add     edx, [ebp+var_7C]
.text:00A65CE4 xor     esi, edx
.text:00A65CE6 mov     [ebp+var_4C], ecx
.text:00A65CE9 xor     ecx, eax
.text:00A65CEB rol     esi, 10h
.text:00A65CEE mov     eax, [ebp+var_48]

```

Figure 75

The encrypted data is written to the file using the WriteFile API:

```

00A6E247 6A 00      push 0
00A6E249 51        push ecx
00A6E24A 8B 4D F4  mov ecx,dword ptr ss:[ebp-C]
00A6E24D 57        push edi
00A6E24E 03 CB     add ecx,ebx
00A6E250 51        push ecx
00A6E251 FF 75 F0  push dword ptr ss:[ebp-10]
EIP 00A6E254 FF D0     call eax
eax:Win
x87SW_SF 0 x87SW_P 0 x87SW_LU 0
x87StatusWord 0000
x87SW_B 0 x87SW_C3 0 x87SW_C2 0
x87SW_C1 0 x87SW_CO 0 x87SW_ES 0
x87SW_SF 0 x87SW_P 0 x87SW_LU 0
Default (stdcall)
1: [esp] 00000308
2: [esp+4] 054C0000
3: [esp+8] 00002000
4: [esp+C] 04C3F6E4
5: [esp+10] 00000000

```

Figure 76

The ".PSFUX" extension is added to the file name:

```

00A7088B 56        push esi
00A7088C FF 75 EC  push dword ptr ss:[ebp-14]
EIP 00A7088F FF D0     call eax
esi:L
eax:MO
x87SW_SF 0 x87SW_P 0 x87SW_LU 0
L"C:\\BOOTSECT.BAK"
L"C:\\BOOTSECT.BAK.PSFUX"
L"C:\\BOOTSECT.BAK"
Default (stdcall)
1: [esp] 030E1C30 L"C:\\BOOTSECT.BAK"
2: [esp+4] 03116ED0 L"C:\\BOOTSECT.BAK.PSFUX"
3: [esp+8] 0300AEB0 L"C:\\
4: [esp+C] 04C3F6CE L"OOTSECT.BAK"
5: [esp+10] 030EFED8

```

Figure 77

The ransom note that is created in every encrypted directory is displayed below:

```

1 All of your files are currently encrypted by CONTI strain.
2
3 As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be recovered by any means without contacting our team directly.
4 If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on the data of the lowest value.
5
6 To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of charge.
7
8 You can contact our team directly for further instructions through our website :
9
10 TOR VERSION :
11 (you should download and install TOR browser first https://torproject.org)
12
13 http://contirec4hbmzyzydyzrv2c65lmvho[REDACTED]onion/
14
15 HTTPS VERSION :
16 https://contirecovery.kxz/
17
18 YOU SHOULD BE AFRAID!
19 Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on our news website if you do not respond. So it will be better for both sides if you contact us as soon as possible.
20
21
22 ---BEGIN ID---
23 UER39kovez8BdoDfom5X9VefqJwJ93e[REDACTED]
24 ---END ID---

```

Figure 78

An example of an encrypted file (file size < 1MB) is highlighted in the next 2 pictures:

```

BOOTSECT.BAK.PSFUX
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 5C 12 56 1C C7 23 B7 0A 56 5C 66 53 C7 06 D6 E1 .V.C#.\fSQ.0á
00000010 5E 0D CD 90 B4 3B 89 68 04 F5 D0 20 B6 48 B5 A3 ^.Í.';th.8D QHuf
00000020 F2 65 1E 51 1C 8E 93 55 32 24 A9 07 B5 25 2D 83 òe.Q.Z*U29@.u%-f
00000030 1E B8 16 1B 74 13 F6 15 87 3B 32 75 8D B2 72 57 .t.ò.+.;2u.^rW
00000040 C4 7D 93 5C 44 0C FA C3 00 51 E2 09 83 F8 58 CC Å)"\D.ú.Á.Qá.føXI
00000050 1E 55 9C 69 8E B3 10 CE CA 24 D0 A5 BF C8 13 84 .UoxiZ'.fESD¥çE..
00000060 B1 4E 37 B7 38 B0 D5 5E 6D B5 98 A5 7A F3 A0 75 ±N7·8°Ô'mu"¥zò u
00000070 55 47 EB 77 13 69 9B 59 66 0C 7E 19 E0 82 11 22 UGëw.i>Yf.~.à..
00000080 69 EA 5A 47 AD 9E D4 A5 25 DB 75 F3 97 55 52 62 ièZG.Z0¥%Ù0-URB
00000090 EE A4 86 B5 76 02 2E AA A0 8E 1B 20 E5 E9 70 D2 imtuv..* Z. áèpò
000000A0 C4 00 A9 06 71 EA 47 86 04 B9 12 5F C7 FA D7 F7 Ä.©.qèG+.². Çux-
000000B0 B7 11 0B 33 CE 88 04 7F C6 55 D1 D2 52 A6 F2 08 .³í'..EUNÖR|ò.
000000C0 BF 05 F9 7D FC 2E 3E 76 CA A8 9A 4A 55 65 A7 D5 ç.ù)ú.>vÈ"§JueSò
000000D0 1D 40 5F 98 91 47 E1 D4 6A DA 07 06 59 BE FA 11 .@_'Gá0jÜ..Ykú.
000000E0 EB 62 EB 6A 4F 37 70 59 F0 A8 D2 27 45 F9 5Ü E2 èbèj07pYè'ò'EùÀá
000000F0 C6 3D FA 70 C7 7C 54 B7 64 07 1F D2 8F D5 1A 2D E=üpÇ|T.d.ò.ò.-
00000100 96 34 B2 7A 5B 54 DB 37 B0 00 5F 28 07 A7 1F BB -4*z[TÜ7°._(.S.)
00000110 92 85 73 E3 77 BC D2 40 7D 14 7D 82 ED 36 92 52 '...sáw*0È|.);iè'R
00000120 F6 42 E0 DE 22 D3 70 B9 A1 A1 41 0B C8 54 09 B9 öBàE"Óp';jA.ÈT.²
00000130 33 46 20 36 40 58 D9 A3 44 37 3B 54 59 CC 1A 4F 3F 6@XUèD7;TYI.0
00000140 0D 7C 06 B4 AF 7D 64 14 DE 4B 09 41 BC 5F C1 A4 .|.')d.BK.A+ÄW
00000150 C8 DC EA D2 5A 3F 10 32 56 79 D4 F2 ED 9E E5 AB EÜè0Z?.2VY0óìZáá
00000160 A7 6B 1B 1B 0F CA E5 78 57 DF 2E 19 FC 1E 90 37 $k...ÈáXWá..ü..7
00000170 F3 59 D6 DF F5 48 7E 95 14 7C 16 CA 82 65 79 AD oYÓB8H~..|.E,ey.
00000180 C5 98 52 DC F5 C2 C4 45 1B C2 88 49 09 1D A4 53 Å"RUèÁÁE.Ä"Í..MS
00000190 E0 F2 B2 C8 DD 51 75 4E 26 C2 2B D2 A1 F3 F6 64 àò=EYQuNçÄ+0;òòd

```

Figure 79

```

BOOTSECT.BAK.PSFUX
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00002000 E7 13 89 A4 F8 58 0B 64 37 54 3D 04 87 5A AB 3F .;kæX.d7T=+.Z«?
00002010 74 0C 78 83 A9 10 15 FD 11 B7 34 A3 64 80 56 0D t.xf@.ý.~4deV.
00002020 3F 46 9B 1B 86 A2 F2 63 A1 8A 05 25 58 72 C1 1E ?F>.toóc;š.æXrÁ.
00002030 C3 8B 22 6B 79 79 75 5A 3E 7C 05 C5 10 76 96 97 Å<"kyyuZ>|ÄÁ.v—
00002040 1D DD CB 0A 96 7C DC C6 62 A7 61 C8 47 4C C9 4E .YÉ.-|ÜEbsaeGLÉN
00002050 92 5B 62 85 DF 23 BE 38 07 09 72 0A AB C6 AD D8 |b..B#*8..r.«E.0
00002060 08 9D B7 DD 33 41 39 25 0D F8 BD B5 E5 33 C3 F1 ..Y3A9%.øµá3Áñ
00002070 A0 ED C6 87 91 15 1F DC 51 E3 4A 98 F6 BE 09 C7 iE+'.ÜQáJ"øk.Ç
00002080 54 74 CE CC 22 8A B5 07 34 0D 08 B4 EE 6B 3D 01 TtÍi"šµ.4..'ik=.
00002090 7D 1D F2 D4 7A FF F1 50 EA 61 BF FB D1 BE EC 63 ).ò0zyñPeazúñkic
000020A0 2C 4B F8 B5 96 EB 34 0E 42 EC EB 38 D8 D4 98 6A ,Kou-e4.Biè800~j
000020B0 02 20 AC 08 59 C8 21 60 47 98 8E 5B 7E AE B6 BF .-.YÈ!'G~Z|~ø¥ç
000020C0 1C 91 9A 98 1F 50 B1 0D 97 EC 51 FE E2 1D 9A D9 .'š".Pt.-iQp.áS
000020D0 EA CC D3 F4 28 B3 7A 53 23 C1 C9 9D 49 BB 51 37 èiÓó('zS#ÁÉ.IæQ7
000020E0 0E 65 BF E1 90 E9 1F 5F 99 68 C8 A1 86 54 AB E6 .eçá.é.._mhÉ;†tæ
000020F0 AA E8 1D F9 F4 77 19 0E C1 24 0A 89 E5 14 BD 09 =è.ùòw..Á$.tá.+.
00002100 15 5D CA E9 F2 0F F5 58 58 D4 4F 96 C5 30 94 BF .]Jèò.öXX00-Ä0"ç
00002110 AE 48 4A 8E 50 7C D6 60 3E B0 8D 38 94 4B DA CD øHJZP|ò>'.8"KÚÍ
00002120 9F 74 A5 28 FE B1 14 DB E3 D9 3A A8 C1 34 BF A9 Ýt¥(pt.ÜÁÜ:"Áç@
00002130 12 DC 57 C7 95 8E E5 8A E5 9D 7C 63 CA 9F DE D6 .ÜWç.ZášÁ.|cèYpó
00002140 66 21 09 38 C1 CF CA 66 1D 9A 64 BA 3E 13 0A 51 f!.sÁIÈf.sd>..Q
00002150 6D 40 2E F7 BB 03 0A 85 40 A6 DF 33 9B 60 C6 57 m@.~>...è;83>`æW
00002160 58 0D F9 BF F5 4B 94 4B F6 64 58 02 9B 52 EA CD X.ùçòK"KòdX.>Réí
00002170 22 59 40 F2 22 14 A0 0F F2 B3 B3 B5 A1 26 67 BB "Y@ò".ò'µ;çg»
00002180 11 DE D0 A7 D2 96 FC EE 2D 66 77 30 C4 0E 5F A8 .FDS0-üi-fw0A..
00002190 ED DB 84 69 5E 75 3A 08 9A E4 15 50 B5 79 AA E5 iÜ.,i^u:.sä.Puy"á
000021A0 91 0E AE 54 D3 4E 0F DE 1E 19 91 3E 4C C7 E8 30 '.@TÓN.F..'>LÇè0
000021B0 BA 86 60 CB 68 03 D0 F4 6F B8 E3 29 EF 7D 3F 4D +†Èh.òó0.á)j?M
000021C0 98 8D D6 25 DC 15 FB 0C 22 8E C0 DE 27 80 32 3A ".òçÜ.á."ZÁB"è2:
000021D0 F9 7A 1A E0 3C 47 B8 54 80 A9 87 8F DA C8 39 84 üz.à<G,TEø+ÜÈ9,.
000021E0 5A 11 7E 65 19 97 90 0F 24 C5 38 FC EE CF 98 36 Z.~e.-..SÁüii"6
000021F0 B9 F0 71 BE AD 64 16 13 60 47 E8 B9 76 9B DC 8A 'èqk.d...Gè'v)Üš
00002200 00 00 00 00 00 00 00 00 00 00 00 24 00 00 20 .....$.
00002210 00 00 00 00 00 00 .....

```

Figure 80

Whether the file size is between 1MB and 5MB and the extension is not in the targeted lists, the ransomware only encrypts the first MB of the file, and the encrypted file has the following structure:

```

test.txt.PSFUX
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00100000 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAA
00100010 F5 39 A3 4F E1 25 32 0E 33 BF FD C9 3E FA C9 09 8940a*2.3yE>uE.
00100020 AF FE BB C6 A7 34 5E 7D 85 F7 3C 10 80 49 D8 39 7p>ES4*)...<.eI09
00100030 99 C8 E1 01 4A E5 95 B4 A5 EB 50 6A B5 32 79 2B "Ea.Ja*'YEPju2y+
00100040 3A FB 64 73 28 0A 7D 15 FD 92 EE C9 B3 EB B2 67 :úds(.).y'iE'e*g
00100050 99 8B 15 77 A7 DB 94 DE 9D 56 7B D3 9E 89 AE 19 "c.wSÜ"b.V(ÖzWø.
00100060 69 FF 02 49 38 41 D0 DF DE 28 20 98 A6 30 5E 12 iy.ISABAB( "l0t.
00100070 1B 05 C3 8E FA 0D 06 91 FE 2D 58 AA E2 80 74 2C .Äžú..p-X'æt,
00100080 A1 2A F5 7D 48 96 0A 60 81 40 AA 40 0C 8C 37 06 ;*õ)H-.'.@*0.E7.
00100090 5C 10 1E 76 05 43 EF 2A A9 1D 4A 27 A6 CF E9 D8 \..v.Ci*@.J';IéÜ
001000A0 74 3F FE 8E 19 62 4E 58 06 0E 8B 31 C5 3B DC 03 t?pž.bnX...<1Ä;Ü
001000B0 A4 5F B8 B8 E3 28 19 83 C2 B3 B3 89 FD D0 E5 BC k...ä.(fÄ*'yDä+
001000C0 7C FA 6B 9E CE 2E 17 7E 82 4A 9F 00 57 06 31 BC |úkkĩ..~.JY.W.14
001000D0 F8 89 77 F4 EB 90 8C 0F 2F 71 99 37 B8 91 BD 90 stwóE.E./qM7.'h.
001000E0 53 4D DE 9C 5A DB 81 0B B8 3F E2 0C 20 C2 0E E8 SmpæZÜ...?ä. Ä.è
001000F0 32 B9 78 E5 3F AA 52 E4 74 02 1F B3 B3 6C 43 FD 2*xä?'Rät...lCý
00100100 70 FD DF EB 04 2E B3 08 C7 13 02 1D 23 46 51 7F pýBé...ç...#FQ.
00100110 31 1B 89 BC 48 03 E5 00 50 2F 0B DF AF C4 E8 A0 1.w+H.ä.P/.B'Äe
00100120 73 3A 2A 38 99 67 6C B1 68 14 FF EC 73 EE AD 2F s:*8mg1th.yis1./
00100130 DC A1 30 7B 71 28 D7 52 32 13 3A A1 B8 12 A9 01 Ü;0{q(*R2.;.;.0.
00100140 9F 46 05 25 2D E8 B6 AE 2B 89 DE DB 29 26 36 7A Yf.%-èq+KpÜ)èz
00100150 09 51 C7 87 65 E7 19 F5 0D F0 C4 1C E2 06 A6 60 .Qç+qç.õ.Ä.ä.;|'
00100160 1F F3 AF 89 B2 ED CA 9B BD 30 D9 D5 9E B4 48 72 .ó'w'iè%ú0Öz'Hr
00100170 08 91 1A EC F0 36 5C B9 D6 8B 11 F9 36 7F A3 39 .'i86\ò.ü.è.6.49
00100180 0A 74 6E AF 7A 50 DA 14 6B 7E E5 97 2D 63 CF 2E .tn-zFÜ.k-ä--cI.
00100190 B4 7A A0 A2 56 BD A6 0C 0E 64 9C 9E E1 28 6A E3 'z cV%|.dæZá(jÄ
001001A0 BA 4E 16 DF 46 C3 93 C5 4C 27 C7 F4 21 79 1F 95 'N.BfÄ'ÄL'çö'y.
001001B0 46 F8 98 4C B7 43 E5 53 3D 86 84 5A F6 32 8E 82 Fø'L.Cás+=,ZøZ2,
001001C0 23 09 68 ED DF 41 1B 4B 85 B1 DC 5A C6 FD 04 70 #.hiBA.K.úZÉy.p
001001D0 AC 8A 72 52 57 FE 59 57 86 62 C1 63 C8 2C 17 7D -ðRrWpYw+baèE..}
001001E0 4E 38 0C 48 26 6B AD 3D FC C6 B4 A9 B1 90 1D DD N8.H&k.=úE'ø+.Y
001001F0 2F D1 E8 F1 DE 88 FF E4 70 DE 36 3C F5 39 2A 2E /ÑèñB'yapB6<89*.
00100200 51 SE 07 53 38 51 81 2B 7F 93 F4 A4 DC 20 89 5B Q'.SQ+.~*6#Ü #[
00100210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....$...
00100220 10 00 00 00 00 00 .....

```

Figure 81

Whether the file size is between 1MB and 5MB and the extension is in the targeted lists, the ransomware encrypts the entire content, and the encrypted file has the following structure:

```

test.sql.PSFUX
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00100000 AA E6 32 1D 07 8C 04 D8 3C BA 07 A4 41 DE CA EC *æ2..E.0<°.wAbEi
00100010 D8 A9 53 62 C0 57 03 83 F1 83 AE FE 40 22 B8 E6 00SbAW.fhfoþ0"æ
00100020 DC C6 D4 A9 B3 B3 F1 A2 8F 07 3A 1B F8 75 80 65 ÜÖ0ë''ñc...ouEe
00100030 35 B3 82 17 95 2A A7 34 08 BA D8 A3 5A 8F DE C5 5',..*$4.°0E2.EÄ
00100040 22 D4 50 60 25 4E AC 05 AA 75 52 0A 3F 4D 5D 9B "ÖP'ñN-.*ur.7M)>
00100050 4C BE 80 23 14 E0 AA 8E 9D 68 94 21 73 35 19 DD Lw#%.ä*ž.h"!s5.Y
00100060 59 CC 49 26 B8 6B 8F FE 1C F6 C4 26 7F 4C B3 76 YII6.k.p.0Äs.L'v
00100070 B6 D3 B5 41 C4 4D 7D 80 35 56 45 CE 3C 68 2B 59 QÓuAÄM)E5VEIç+Y
00100080 C0 90 D8 A3 CD 81 0A B7 ED EB 71 A2 94 24 51 A6 Ä.0EÍ..ieqç"SQ;
00100090 BE 94 A0 20 97 DE 87 F3 8F 99 B3 8E A1 78 2E 0E %" -B+ó.™ž;xç.
001000A0 80 ED E8 12 D4 77 6D 66 1C AD E5 11 D0 5D F2 9F eie.öwmf.ä.ð]óY
001000B0 4C 5C FB 36 E4 B5 45 1D B9 23 F4 52 E3 74 30 09 L\ú6äU.E.'#6Rät0.
001000C0 4A BD 6D 24 DB DF 9F A9 B7 AD D9 A7 92 08 DF 8D J=msÜBÿe..Üs'.B.
001000D0 92 DD 2A 11 66 63 B2 0A 92 FD CC 43 1E 22 D0 87 'Y*.rc'.yIC.'#B+
001000E0 61 C9 95 3A 8A E5 3B 25 FA 8D 08 E3 E8 48 4E 60 aE':Sä;ú..äèHN'
001000F0 EB BD B2 EF 3D 95 0C 58 1B 4D 42 49 C0 28 45 A5 è%:i=-.X.MBIÄ(EW
00100100 D2 1C B7 37 E1 57 9A D3 6E 42 DC DA 1D 0C 9F 6B Ö.7ÄW8OnBÜÜ..(Y
00100110 D8 56 A4 8B 35 AA B2 B4 BC 63 38 44 F7 14 56 CF 0VW<5*~4c8D+.VÍ
00100120 54 45 32 9C A9 F0 39 7B 51 F3 7D 28 EF 2B D3 36 TE2ø089(Q6)(i+0ç
00100130 12 F6 42 28 F0 32 70 89 57 FB AF F5 9E 64 C7 E4 .8B(82ptWü'õzdÇä
00100140 0B BD 53 7F 56 F6 DE E3 84 B4 88 1B 9F A9 33 D7 .4s.VoPÄ..'.Ie8x
00100150 5C 82 1B 1A 4B CD 29 01 FD 22 F9 D9 98 5F 7E D7 \,..KI).y"üÜ-~x
00100160 16 E2 66 49 E0 BC 93 D7 99 B0 35 CC B0 69 4D FA .äfiÄ4"™™5i'iMü
00100170 C3 91 8D C6 E5 F7 72 FB 37 BB A7 BC 91 B3 0C 7F Ä'.EÄ-rÜ7s94'..
00100180 23 10 14 64 7B 3A 05 11 3B 97 E7 AC 9F 31 9C A0 #.d{...;ç-YIoe
00100190 B8 98 FA 61 B0 B1 E7 9A 48 D7 4B 9D 9D 16 A9 27 .üa'tçðHxK..0'
001001A0 DD 54 4D 6B D7 0A 92 D4 E0 EA 26 B1 A3 56 C0 2E YTMkx.'Öä&±fVÄ.
001001B0 81 28 E2 FE 43 30 17 64 DE 87 FB 1A 30 E3 18 37 .(äpCO.dp#ü.0Ä.7
001001C0 35 00 7C 94 C8 A6 77 5E 33 A7 A8 5F 35 84 85 09 5.|"Eiw'3S'_5....
001001D0 29 FD CD 52 08 A3 CC 95 60 15 E2 1B AA 68 17 37 )YIR.äi'.ä.'h.7
001001E0 04 2E D2 77 F8 FF 14 13 CD DE 0C B2 CC 33 CA 34 .Öwøy..iB.'i3E4
001001F0 15 31 B2 0A 73 B5 AD A5 12 61 66 75 70 55 87 95 .1s.sp.w.afupU+
00100200 AC 1A 9A 86 2C 80 17 B3 46 D3 84 A8 DA 0B B8 BB ~.ät,e'.FÖ."Ü..»
00100210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....$...
00100220 10 00 00 00 00 00 .....

```

Figure 82

Whether the file size is greater than 5MB and the extension is not in the targeted lists, the ransomware encrypts 5 chunks of (file size/100 * 10) bytes. In this case, this value is (0x500010/0x64 * 0xa) = 0x7FFF8 bytes (basically, the malware encrypts 0x7FFF8 bytes, then skips some bytes, and then encrypts 0x7FFF8 bytes again and so on). The structure of the encrypted file is presented below:

```
test.bt.PSFUX
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0007FF50 20 27 38 E0 A3 15 77 A8 D4 D1 E9 AD 8F C2 BD 63 '8az.w'ÖÑé..Â%c
0007FF60 58 DB 94 0C 99 26 47 D8 F5 96 74 84 11 02 70 D3 XÜ".%&G06-t...pO
0007FF70 13 19 5B 15 FC BF 17 A5 3B 1F F9 F1 0C F2 79 63 ..[.úç.¥; ùñ.òyc
0007FF80 D9 15 CD F6 30 66 68 BE 2E BF A9 D3 1B 27 4A 96 Û.Íó0fhk.¿ó.°'J-
0007FF90 38 EA D9 1C 68 2F 2D 37 85 47 E6 F5 24 62 48 65 8èÛ.h/-7...Gæ5öbHe
0007FFA0 00 27 8E 6C 45 88 C2 26 36 35 1E 45 EA AF BC 0E .'ZlE^Å.65.Eë"4.
0007FFB0 22 45 B1 27 CE E4 DD 12 38 13 1A 7B 23 63 6A 6D "E±'IáY.8..{#cjm
0007FFC0 F6 12 84 24 92 27 63 E6 76 5A 68 84 79 C3 FA D2 ö.,$'cævZh,,yÅúÖ
0007FFD0 19 6B D1 4D 8D FC C1 43 F7 C2 D0 7F 9C 3F 5E 49 .kNM.úÁc-ÁD.ø?^I
0007FFE0 08 5A 88 B5 F2 08 79 06 34 7A 7E 6D C7 26 64 43 .Z^µò.y.4z~mÇ&cC
0007FFF0 81 3D F8 92 6A 75 7C EA 41 41 41 41 41 41 41 41 .=ø'ju|èAAAAAAAA
00080000 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAA
```

Figure 83

```
test.bt.PSFUX
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
004FFFE0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAA
004FFFF0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAA
00500000 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAA
00500010 95 F5 46 25 C5 B8 F7 BA C7 CA 6A 94 09 0B B0 62 *ðF%Á,-°ÇEj"...°b
00500020 2F 28 EE 52 17 3C 63 FA C1 9C 46 F8 ED B2 92 5B /(iR.<úÁøFøi'á'[
00500030 76 C4 91 7A 79 00 79 C5 50 22 99 5F D5 16 C2 69 vÅ'zy.YÁP"™.ø.Ö.
00500040 17 90 20 12 4A 72 10 E4 DF BD 35 3F C0 DA 32 3B ..Jr.äB*5?ÁÚ2;
00500050 06 06 DF B0 B0 E6 F9 40 50 56 4D 55 17 B9 69 2B ..B°ø@PVMU.°i+
00500060 05 00 79 21 65 F1 5C 95 51 8E CA C2 C2 D3 75 C3 ..y!eñ\°QZÈÁÁóuÅ
00500070 48 33 C3 5D 14 21 4D 46 8F AF B8 F0 83 83 40 25 H3ÅJ.!MF.°,øff@%
00500080 B9 01 22 29 CA D9 DD C3 F9 F5 2C 07 11 0D 9C B5 ".")ÈÜYÀùò,...øµ
00500090 F4 BB 61 12 DD 03 D1 D6 FE 28 94 E5 8C 21 25 74 ówa.Y.NÖp ("ÁC!%t
005000A0 8B 1F 60 95 0A 38 DC 8C 02 CE 07 7C CB D4 CA 7C <..°.8Üø.Í.|ÈÖÈ|
005000B0 C2 BE 24 18 32 87 40 B5 43 A9 EE 41 37 42 89 A0 Å%$.2+@µC@iA7B%
005000C0 E1 03 13 CC 85 92 46 12 68 DA 41 30 4D F8 98 B7 á..ì.'F.hUÁOMø'
005000D0 95 79 1F 26 F3 06 22 E5 E7 7A E5 C9 44 7B DC 6E .y.óó."áçzãÈD(Ûn
005000E0 B8 EC F7 8D 1B 81 D5 47 CE A6 F1 6D A9 B6 C5 0E .i+...ÖGI;ñmøqÁ.
005000F0 9F CF E3 B7 19 4C F8 52 35 60 36 25 99 D9 4A 16 ÝIã..LøR5'6%™ÜÖ.
00500100 93 5D 96 14 4F 2F 8A A0 32 F3 9C 1B C0 C8 D7 41 "]-.O/Š 2óø.ÀÈ×A
00500110 26 61 D9 14 6D 34 9D 36 96 22 D7 06 87 46 78 68 6aü.m4.6-"×.+Fzh
00500120 F2 51 E5 28 06 AB EF 43 D3 24 39 BA E0 8B BB 55 òQã(.<¡CÓ$9°à<»U
00500130 C7 6D F3 0D AF E2 1C 54 19 4A C1 A9 22 2F 50 89 Çmó.ª.T.JÁø"/P%
00500140 1A 31 14 CE EF C9 1E 0D 29 D4 40 07 43 F1 F5 FB .l.ÍiÉ..)Öø.CÁóú
00500150 37 B3 80 03 E9 C0 DE 59 C7 2E 95 F2 53 84 10 26 7*è.éÀBYÇ.°óS,,&
00500160 44 1E 61 77 58 D3 CC 2F 0E CE 87 06 A5 20 64 2E D.awXÓi/.í+.¥ d.
00500170 D7 D4 83 04 DA C0 24 77 AE 1E 48 D1 11 14 1B 34 *Öf.ÜÁ$wø.HN...4
00500180 7B 5C 2F CF E9 D4 CB 6D 74 F6 96 74 03 53 B3 38 {/IéÖEmtö-t.S°8
00500190 E7 D2 8A 08 FB 10 6F C6 0C EB 18 CE 60 A7 B5 FD çóŠ.ú.øE.è.í'šuy
005001A0 CE 87 76 E9 C7 B4 52 4D FB 9F 1F 8D 5D FB FA B5 Í+véÇ'RMÛY..]úúµ
005001B0 8B EF D4 65 0A 52 4E C7 09 90 A7 87 0F 5D 17 78 <iöø.RNÇ..$+.]x
005001C0 A6 C8 57 F6 E7 A2 9A 1B 22 F8 F0 0E 8D 22 55 48 |ÈWöçóš."øø.."UH
005001D0 83 80 4D AE EB 17 3F 28 8E F9 96 43 92 F0 0C 16 fèMøø.?(Zù-C'ø.
005001E0 DE 95 76 A6 DA CE 81 DA C4 37 7D 17 8F 7D 72 8C E+v;Úí.ÚÁ7)..}xø
005001F0 0D 49 E1 19 88 84 90 06 C0 32 55 F6 F2 12 74 34 .Iá.^,..À2Uóò.t4
00500200 8C A4 D9 9E 6D 19 DA 3C 60 D1 F9 16 52 09 9E 99 ÇUžm.U<'Nù.R.ž™
00500210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....%2..
00500220 50 00 00 00 00 00 P.....
```

Figure 84

Whether the file size is greater than 5MB and the extension is not in the targeted lists, the ransomware encrypts the entire content, and the encrypted file has the following structure:

```

test.sql.PSFUX
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
004FFFE0 67 4F 91 00 8E DA 9D 96 D3 86 BC 1D E9 B5 74 FC gO`.ZÜ.-ó+*.éutú
004FFFF0 51 C0 98 6B 07 7D 2A 7C 98 CA 20 C1 E9 9E 79 49 QÀ`k.)*)|`È ÁézyI
00500000 10 0C D0 4C F2 05 10 59 D6 D9 70 F4 02 88 A7 EB ..ĐLò..YÖUpó.ˆŞè
00500010 B1 F9 17 D1 39 14 BB 2F A7 B2 13 8F D9 3D 56 8C àù.Ñ9.„/Şˆ.Ù=VE
00500020 26 40 2A E7 04 BD 39 C0 47 6E BD 4D 4E DC 86 80 s@ˆç.ˆ9AGnˆMNÙ+e
00500030 DC 7A 4D BF C0 E2 33 DD B4 18 92 3D C4 2B 81 FB ŪzMçÁá3Yˆ.ˆ=Á+.ù
00500040 73 22 5C EC 0C E3 7E 94 6A 4E EB AA 95 A0 4D 0F s"ˆ\i.á~"jNéˆˆ M.
00500050 0D 5B B7 0D 18 4B C1 E3 45 17 0C 10 EE 2C 18 4C .[ˆ. .KÁÈE...i.,L
00500060 CA 52 FD 63 EE 98 5F 3D AE 16 B4 C7 F3 A3 46 7F ÈRýciˆ" =@.ˆÇóèF.
00500070 84 43 B9 AA BA 22 08 79 1C 57 A1 54 10 AB 60 E0 „Cˆˆˆˆ.ˆy.WjT.«ˆà
00500080 92 3C 6E 1E DC 17 18 F3 9B 32 B7 4B 3F 60 F8 BA 'ˆ<n.Ū.ˆ.ó2`K?ˆˆ°
00500090 B5 66 35 3A F9 83 D1 E6 48 51 A1 E2 CF 60 D8 8C pf5:ùfÑèHQ;áIˆØE
005000A0 0D D6 70 60 77 15 E4 05 DD 5B F3 F8 46 EB 96 F8 .Ópˆw.á.Ÿ[óøFè-ø
005000B0 EA A5 FA CA A2 8F 73 AB 9C 04 65 C9 00 CB 7F 2C èVúÈc.sæ.e.È.È.
005000C0 A0 F0 AA 35 FB F3 3F 7E B8 C3 AE A5 4D D9 F1 08 øˆ5úó?ˆ.ÁøWUñ.
005000D0 45 B2 13 DB A4 88 2C F0 02 3A 08 59 AA 22 B5 58 Eˆ.Ūwˆ.ø.ˆ.Yˆ"uX
005000E0 6C 72 92 F7 AC 5C 42 D2 2F 8A 87 81 61 58 CE B7 lr'ˆ+ˆ\B0/Š+.aXíˆ.
005000F0 12 38 62 F1 7D B6 DA 46 48 5F 64 DD DB 71 76 98 .8bã}qÚFH dYÚqvˆ
00500100 79 6A D3 D8 2E 8A 76 99 F0 D9 79 79 2D F3 2B 19 yjÓó.ŠvˆøŪyy-ó+.
00500110 FA 12 3C F2 73 0D B6 40 82 B1 44 48 EF 74 41 86 ú.ˆ<bs.Ÿ@.ˆDHItAt
00500120 E9 E0 87 74 C0 2C 32 F7 85 03 AD CB F6 C5 3F 5B éá+Á,2ˆ.....ÈóÁ?{
00500130 1F 6C E8 4A 69 74 45 A5 6C 66 8F 7A CB EC 6B 82 .leJitEYlf.zÈik,
00500140 E9 8E 04 F3 A2 05 32 EC 1C 15 64 D8 D2 A0 8B C7 éž.ó.c.2i.ˆd00 <Ç
00500150 A3 61 9E 88 75 27 42 E2 4F B1 E9 73 31 0A 85 B8 éazˆuˆBÁó+és1....,
00500160 EE 8F 8A 3B DB 21 17 BD BF 2A CC 20 9E FE 21 BB i.Š;Ū!..ˆzçˆI žp!ˆ»
00500170 C9 02 0E 7B 62 C8 97 27 69 E8 D1 20 F3 08 F0 E0 È.ˆ{bÈ-ˆièN ó.óà
00500180 59 06 81 4E 05 03 B4 40 8F 16 4D 31 C7 20 7B CF Y.N...ˆ.È.M1Ç (i
00500190 D3 01 0A E9 14 58 35 5F 72 73 EB 75 18 79 96 56 Ó.ˆ.é.X5_rseu.y-V
005001A0 F9 48 EA 99 5F 32 69 62 9F 8C A2 ED A8 1C 63 2C ùHè™_2ibYGeiˆ.ˆc.
005001B0 45 CD 88 A6 29 17 88 C3 64 74 9A F6 BF F0 80 11 EÍˆ!ˆ).ˆÁdtšóçøe.
005001C0 69 34 12 B0 EB C7 45 6E 6A F3 6E 10 C9 87 9D 72 i4.ˆe@Enjón.Èˆ.r
005001D0 57 F8 E7 FE E0 36 38 66 94 E7 9D 9A 28 DA 5E D0 Wøçpá68fˆˆç.š(ŪˆD
005001E0 35 22 13 BF A4 42 0E 08 47 86 7C 22 24 D8 DA A0 5".ˆz#B..G+|"ŞóŪ
005001F0 CE 2D 8B FE A0 B1 F4 FE 29 2E 74 FE CA 1C 65 3D Í-ˆ<p +óþ).tpÈ.e=
00500200 D3 3B 80 DD 09 15 8C AC A9 58 AD 6A 59 4A A2 00 Ó;èY.ˆ.Ç-èX.jYJc.
00500210 00 00 00 00 00 00 00 00 00 00 00 24 00 10 00 .....S...
00500220 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 P.....

```

Figure 85

When the malware runs with the "-log" parameter, then the list of actions is logged in a file:

```

test.log x
1 [08:19:53] Found 2 drives:
2 [08:19:53] C:\
3 [08:19:53] D:\
4 [08:19:58] Can't get file size C:\$WINRE_BACKUP_PARTITION.MARKER. GetLastError = 0
5 [08:19:58] Can't open file C:\bootmgr. GetLastError = 5
6 [08:20:02] File C:\Program Files\██████████.int is already open by another program.

```

Figure 86

APPENDIX

Lists of targeted extensions:

- .4dd .4dl .accdb .accdc .accde .accdr .accdt .accft .adb .ade .adf .adp .arc .ora .alf .ask .btr .bdf .cat .cdb .ckp .cma .cpd .daccpac .dad .dadiagrams .daschema .db .db-shm .db-wal .db3 .dbc .dbf .dbs .dbt .dbv .dbx .dcb .dct .dcx .ddl .dlis .dp1 .dqy .dsk .dsn .dtsx .dxi .eco .ecx .edb .epim .exb .fcd .fdb .fic .fmp .fmp12 .fmpls .fol .fp3 .fp4 .fp5 .fp7 .fpt .frm .gdb .grdb .gwi .hdb .his .ib .idb .ihx .itdb .itw .jet .jtx .kdb .kexi .kexic .kexis .lgc .lwx .maf .maq .mar .mas .mav .mdb .mdf .mpd .mrg .mud .mwb .myd .ndf .nnt .nrmlib .ns2 .ns3 .ns4 .nsf .nv .nv2 .nwdb .nyf .odb .oqy .orx .owc .p96 .p97 .pan .pdb .pdm .pnz .qry .qvd .rbf .rctd .rod .rodx .rpd .rsd .sas7bdat .sbf .scx .sdb .sdc .sdf .sis .spq .sql .sqlite .sqlite3 .sqlitedb .te .temx .tmd .tps .trc .trm .udb .udl .usr .v12 .vis .vpd .vvv .wdb .wmdb .wrk .xdb .xld .xmlff .abccdb .abs .abx .accdw .adn .db2 .fm5 .hjt .icg .icr .kdb .lut .maw .mdn .mdt
- .vdi .vhd .vmdk .pvm .vmem .vmsn .vmsd .nvram .vmx .raw .qcow2 .subvol .bin .vsv .avhd .vmrs .vhdx .avdx .vmcx .iso