Swascan

TINEXTA GROUP

Cactus Ransomware: analisi malware

www.swascan.com

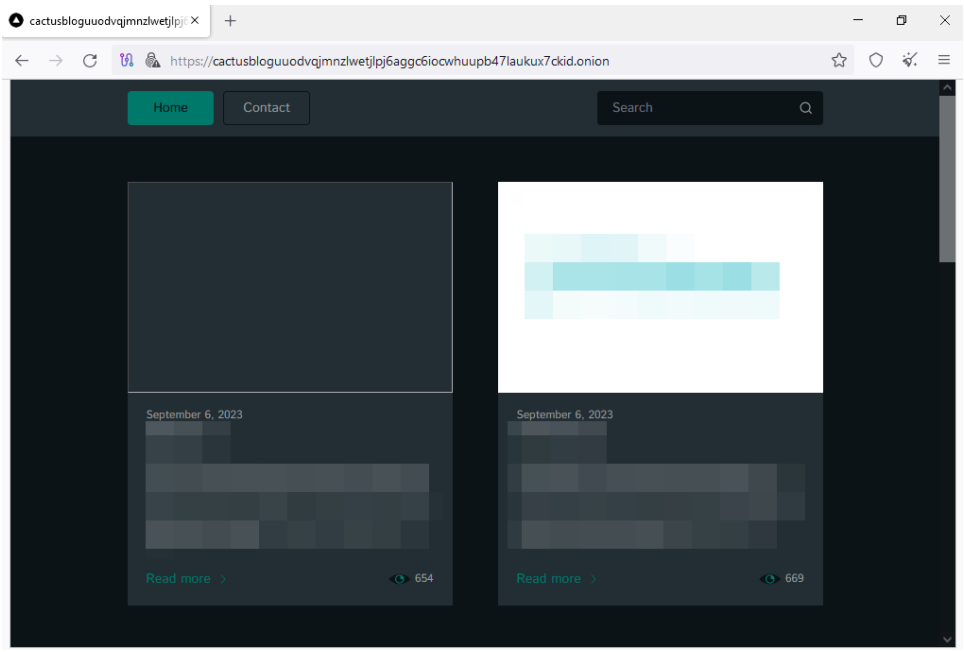
Elementi importanti dell'analisi:

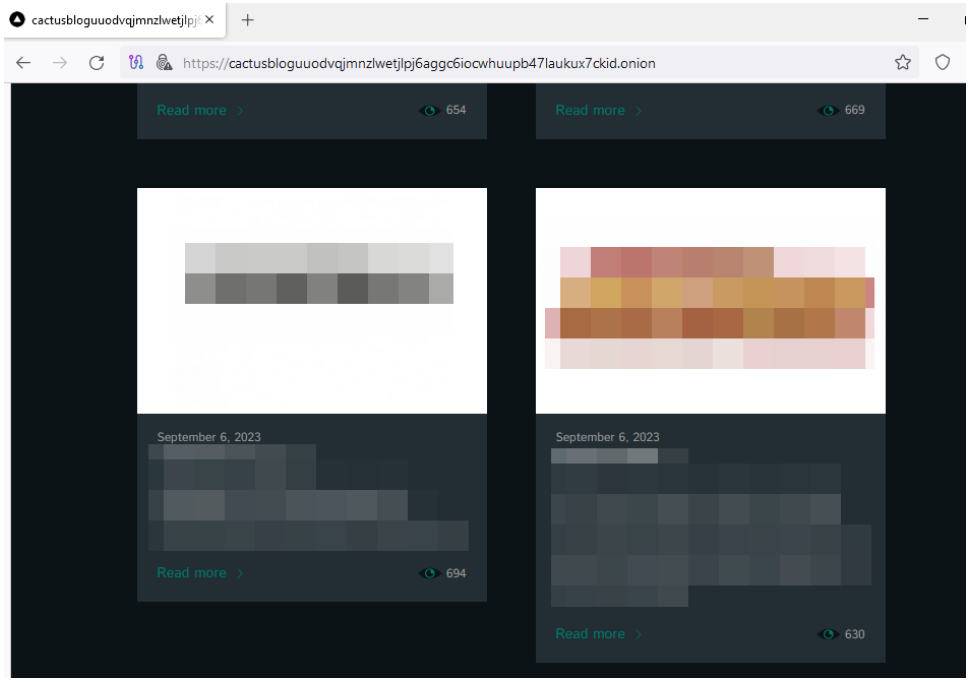
- Attack vector con vulnerabilità Fortinet VPN
- Auto-encryption del ransomware stesso per effettuare bypassing
- Cambio dinamico e consecutivo delle estensioni dei files criptati
- UPX packing
- Algoritmi OpenSSL, AES OCB, ChaCha20_Poly1305
- Scheduled tasks
- Esecuzioni di restart management
- Enumerazioni shares di rete
- Utilizzo del file C:\ProgramData\ntuser.dat per la chiave pubblica dell'auto-encryption
- Crittografia dei files in "buffers"

Introduzione

Cactus Ransomware è una nuova minaccia, identificata per la prima volta nel Marzo 2023, con alcune caratteristiche particolari. Viene distribuita nelle infrastrutture compromesse utilizzando principalmente come attack vector alcune vulnerabilità di Fortinet VPN che permettono un accesso non autorizzato. La caratteristica principale di questo ransomware è l'auto-encryption, ovvero la cifratura del medesimo avviene contestualmente alla fase di deployment e questo comporta il fatto che il threat non possa essere rilevato facilmente da EDR, XDR e antimalware. Durante il processo di encryption dei files target vengono modificate in modo dinamico le estensioni utilizzate, passando da *.cts0* a *.cts1*. Durante la fase di esecuzione il malware controlla, similmente a ciò che avviene in un accesso concorrenziale, se un file è accessibile in un determinato momento o meno.

Il sample possiede il portale di data leak hxxps[://]cactusbloguuodvqjmnzlwetjlpj6aggc6iocwhuupb47laukux7ckid[.]onion, il quale contiene i dettagli delle varie vittime e dei dati ad esse relativi.





I canali di comunicazione dei malcoders risultano essere principalmente l'indirizzo e-mail cactus[@]mexicomail[.]com e la TOX Chat avente URL hxxps[://]tox[.]chat[/):]7367B422CD7498D5F2AAF33F58F67A332F8520CF0279A5FBB4611E0121AE421AE1D49ACEABB254686

Dando uno sguardo approfondito alle modalità di infezione e deployment di Cactus Ransomware appare evidente che esso predilige perlopiù aziende di grandi dimensioni e con un elevato fatturato annuale, con lo scopo, molto probabilmente, di massimizzare il guadagno illecito derivante dalle azioni di riscatto. Quattro grandi aziende recentemente colpite da infezioni Cactus Ransomware fanno riferimento ad attività di private equity, produzione di attrezzi idraulici e cilindri pneumatici, produttori di porte e cancelli, nonché di riscossione debiti. Altre aziende vittime meno recenti riguardano i settori di: agenzie immobiliari, formazioni specialistiche sui trasporti, industry mining e financing, produttori di rimorchi e trasformazione alimentare.

Facendo riferimento a scenari real-world si ha contezza delle seguenti peculiarità chiave:

- Utilizzo dei tools seguenti: Chisel (per effettuare connessioni C&C ed eseguire comandi a bordo delle macchine infette in modalità stealth), Rclone, TotalExec
- Utilizzo del tool SoftPerfect Network Scanner per effettuare discovery dell'infrastruttura target

- Comandi PowerShell per identificare gli hosts di dominio, eventi di login 4624 per identificare le varie utenze
- I tools di remote management maggiormente utilizzati da Cactus Ransomware sono i seguenti: Splashtop, AnyDesk e SuperOps RMM
- Esecuzioni di scripts batch con il fine di disinstallare security solutions ed antimalware products
- Dumping di credenziali LSASS con il fine di effettuare tasks di privilege escalation all'interno del dominio

[1]

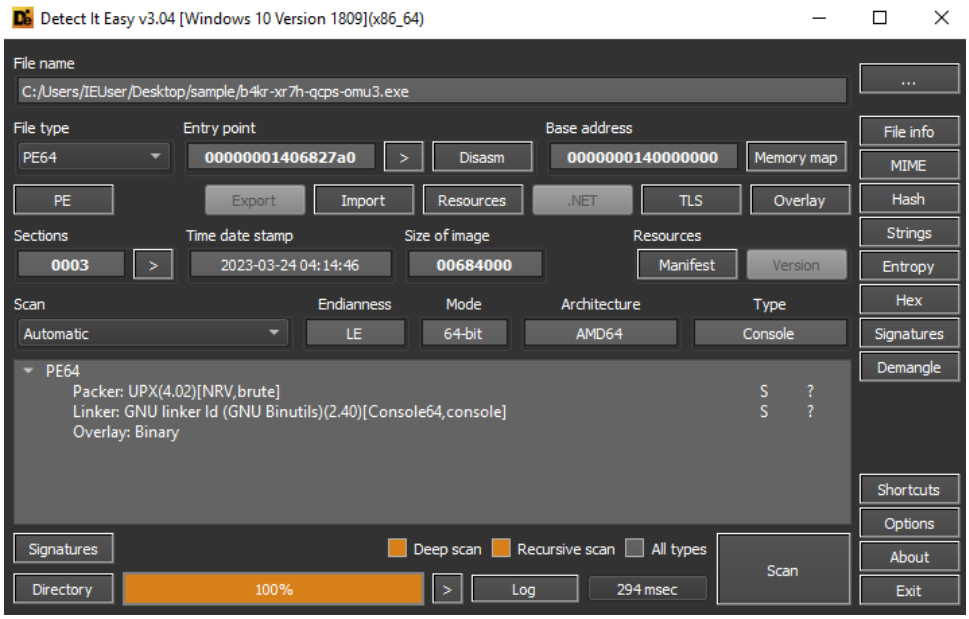
Matrice MITRE:

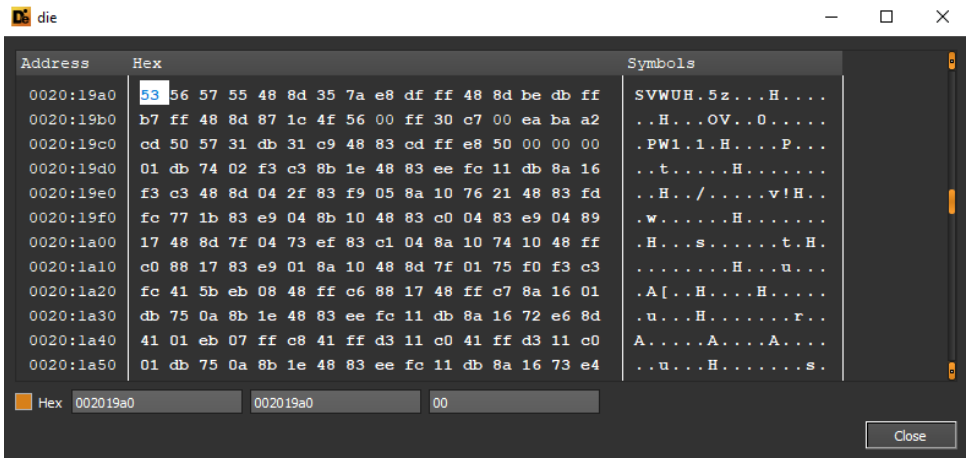
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Software Packing	OS Credential Dumping	1 System Information Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

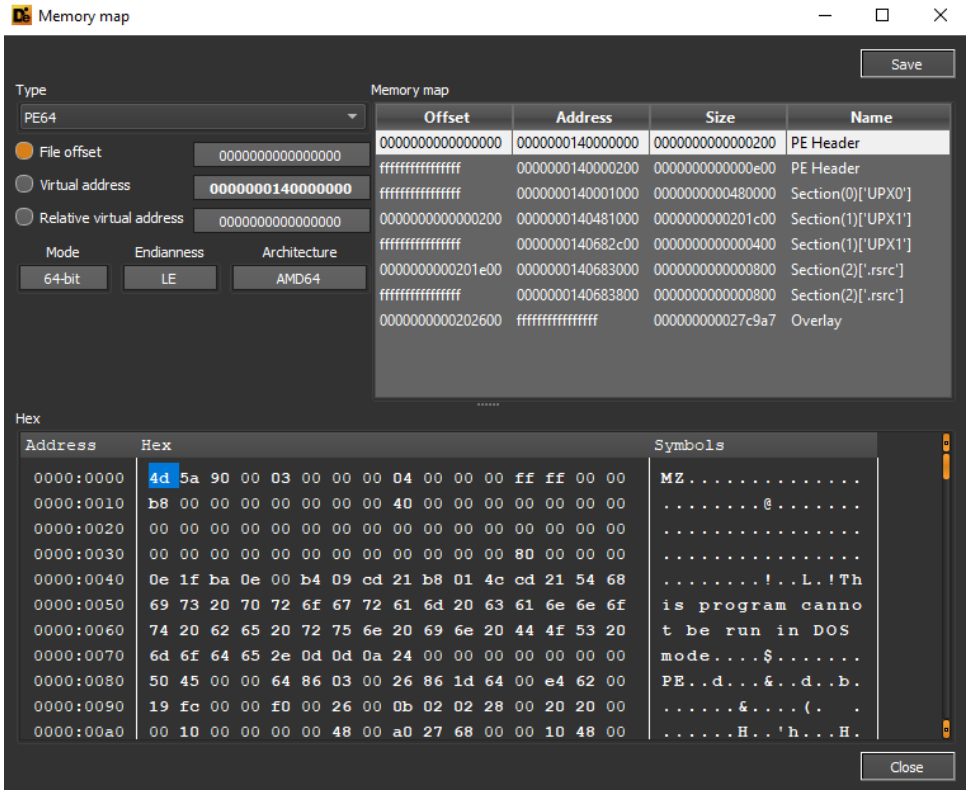
Analisi statica ed assessment

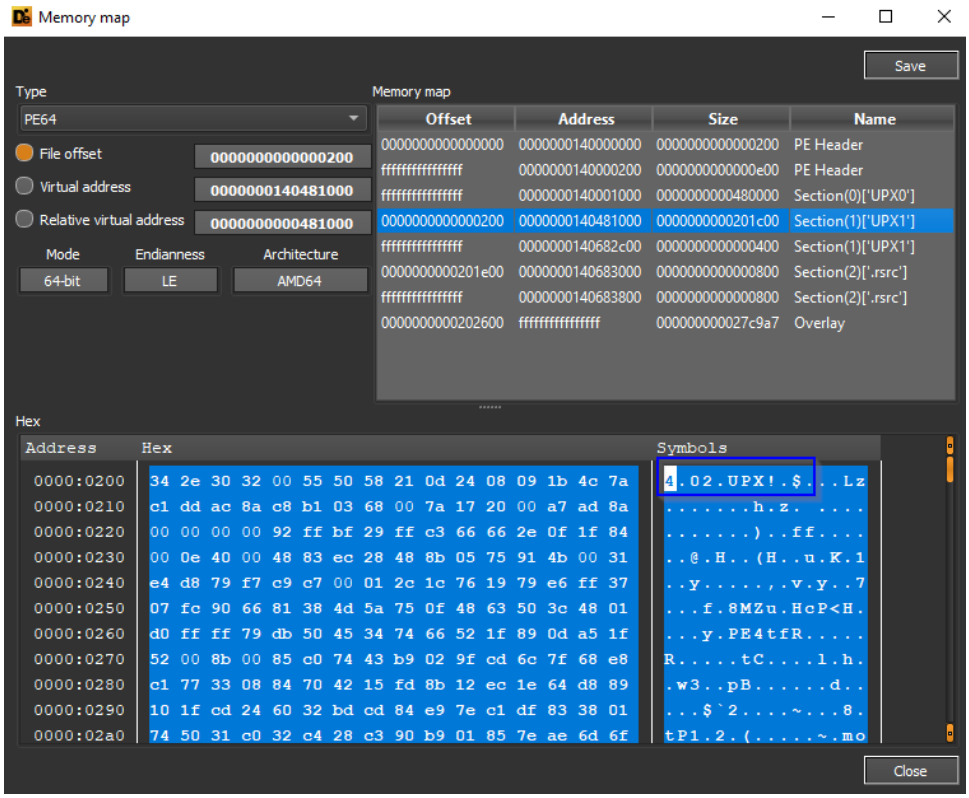
Il sample sottoposto ad analisi ha come hash **78c16de9fc07f1d0375a093903f86583a4e32037a7da8aa2f90ecb15c4862c17**, esso è in stato di packed con il packer *UPX*.



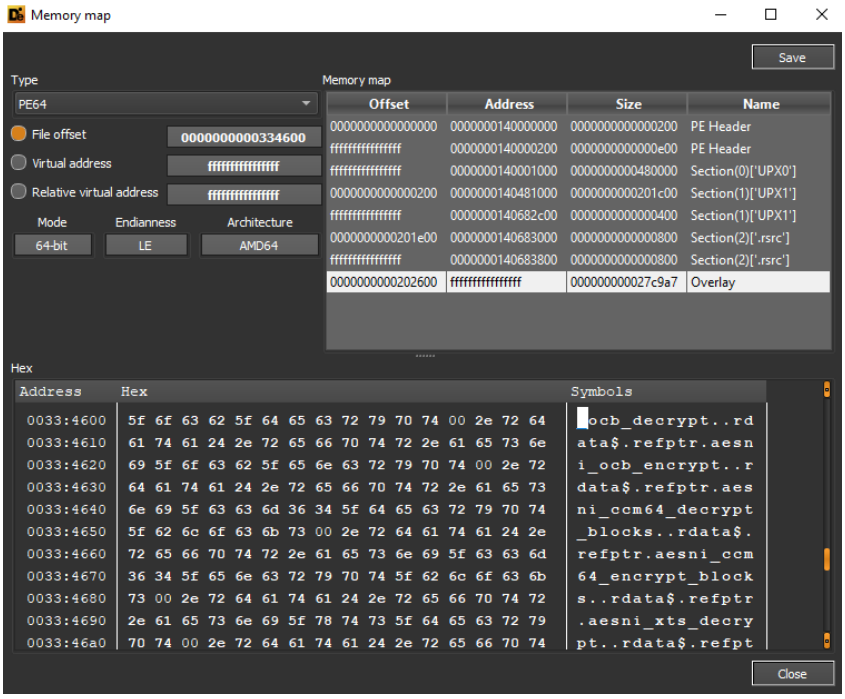


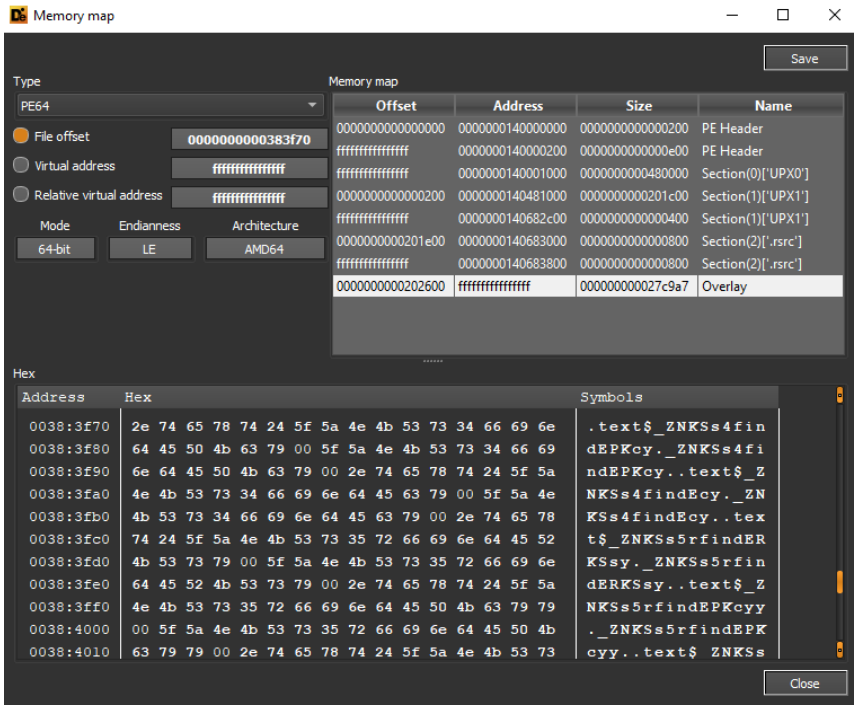
Di seguito i dettagli delle sezioni del file, ove si evincono le caratteristiche delle sezioni relative al packer UPX e *.rsrc*.


Memory map
Save
Type
PE64
File offset
0000000000000000
Virtual address
0000000140000000
Relative virtual address
0000000000000000
Mode
64-bit
Endianness
LE
Architecture
AMD64
Memory map
Offset
Address
Size
Name
0000000000000000 0000000140000000 0000000000000200 PE Header
ffffffffffffffff 0000000140000200 0000000000000e00 PE Header
ffffffffffffffff 0000000140001000 0000000000480000 Section(0)['UPX0']
0000000000000200 0000000140481000 0000000000201c00 Section(1)['UPX1']
ffffffffffffffff 0000000140682c00 0000000000000400 Section(1)['UPX1']
0000000000201e00 0000000140683000 0000000000000800 Section(2)['.rsrc']
ffffffffffffffff 0000000140683800 0000000000000800 Section(2)['.rsrc']
0000000000202600 ffffffffffffffff 000000000027c9a7 Overlay
Hex
Address
Hex
Symbols
0000:0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..............
0000:0010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ....@.......
0000:0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0000:0030 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 ....
0000:0040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ....!..L.!Th
0000:0050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is program canno
0000:0060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t be run in DOS
0000:0070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$.......
0000:0080 50 45 00 00 64 86 03 00 26 86 1d 64 00 e4 62 00 PE..d...&..d..b.
0000:0090 19 fc 00 00 f0 00 26 00 0b 02 02 28 00 20 20 00 ......&....(. .
0000:00a0 00 10 00 00 00 00 48 00 a0 27 68 00 00 10 48 00 ......H..'h...H.
Close

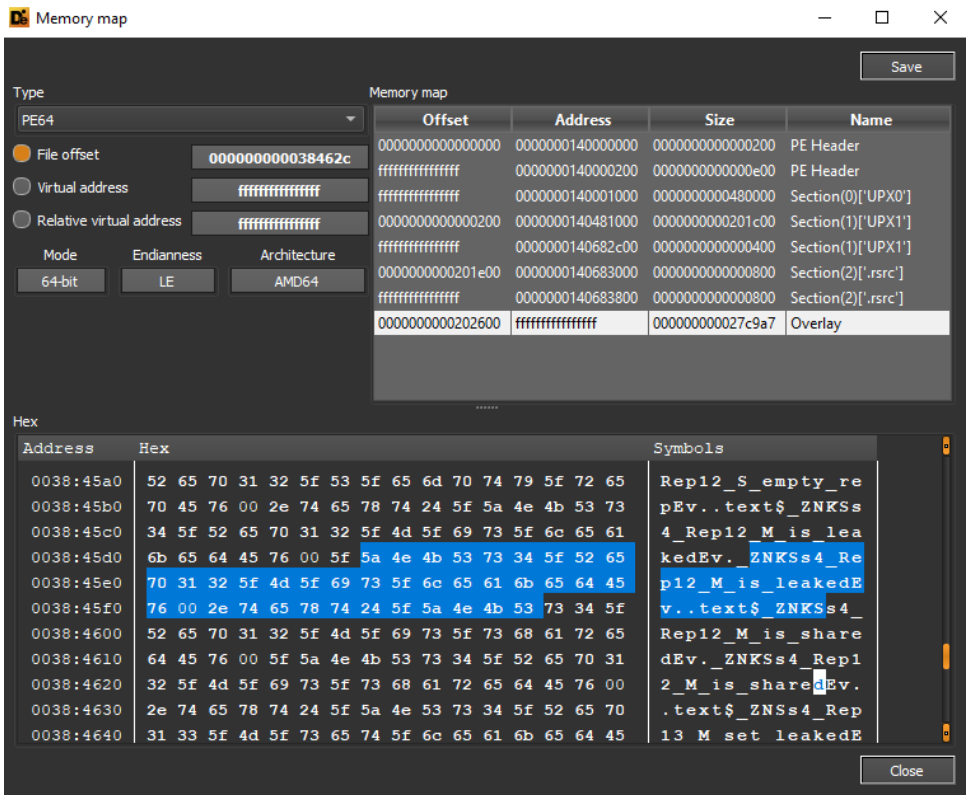

Memory map
Save
Type
PE64
File offset
0000000000000200
Virtual address
0000000140481000
Relative virtual address
0000000000481000
Mode
64-bit
Endianness
LE
Architecture
AMD64
Memory map
Offset
Address
Size
Name
0000000000000000 0000000140000000 0000000000000200 PE Header
ffffffffffffffff 0000000140000200 0000000000000e00 PE Header
ffffffffffffffff 0000000140001000 0000000000480000 Section(0)['UPX0']
0000000000000200 0000000140481000 0000000000201c00 Section(1)['UPX1']
ffffffffffffffff 0000000140682c00 0000000000000400 Section(1)['UPX1']
0000000000201e00 0000000140683000 0000000000000800 Section(2)['.rsrc']
ffffffffffffffff 0000000140683800 0000000000000800 Section(2)['.rsrc']
0000000000202600 ffffffffffffffff 000000000027c9a7 Overlay
Hex
Address
Hex
Symbols
0000:0200 34 2e 30 32 00 55 50 58 21 0d 24 08 09 1b 4c 7a 4.02.UPX!.$...Lz
0000:0210 c1 dd ac 8a c8 b1 03 68 00 7a 17 20 00 a7 ad 8a ....h.z. ....
0000:0220 00 00 00 00 92 ff bf 29 ff c3 66 66 2e 0f 1f 84 ....)..ff....
0000:0230 00 0e 40 00 48 83 ec 28 48 8b 05 75 91 4b 00 31 ..@.H..(H..u.K.1
0000:0240 e4 d8 79 f7 c9 c7 00 01 2c 1c 76 19 79 e6 ff 37 ..y.....,.v.y..7
0000:0250 07 fc 90 66 81 38 4d 5a 75 0f 48 63 50 3c 48 01 ...f.8MZu.HcP<H.
0000:0260 d0 ff ff 79 db 50 45 34 74 66 52 1f 89 0d a5 1f ...y.PE4tfR.....
0000:0270 52 00 8b 00 85 c0 74 43 b9 02 9f cd 6c 7f 68 e8 R.....tC....l.h.
0000:0280 c1 77 33 08 84 70 42 15 fd 8b 12 ec 1e 64 d8 89 .w3..pB......d..
0000:0290 10 1f cd 24 60 32 bd cd 84 e9 7e c1 df 83 38 01 ...$`2....~...8.
0000:02a0 74 50 31 c0 32 c4 28 c3 90 b9 01 85 7e ae 6d 6f tP1.2.(.....~.mo
Close

All'interno della sezione *Overlay*, che contiene dati "appended" all'immagine del Portable Executable, vi sono riferimenti a funzioni di encryption come, ad esempio, *ocb_decrypt* e la sezione *.rdata*.

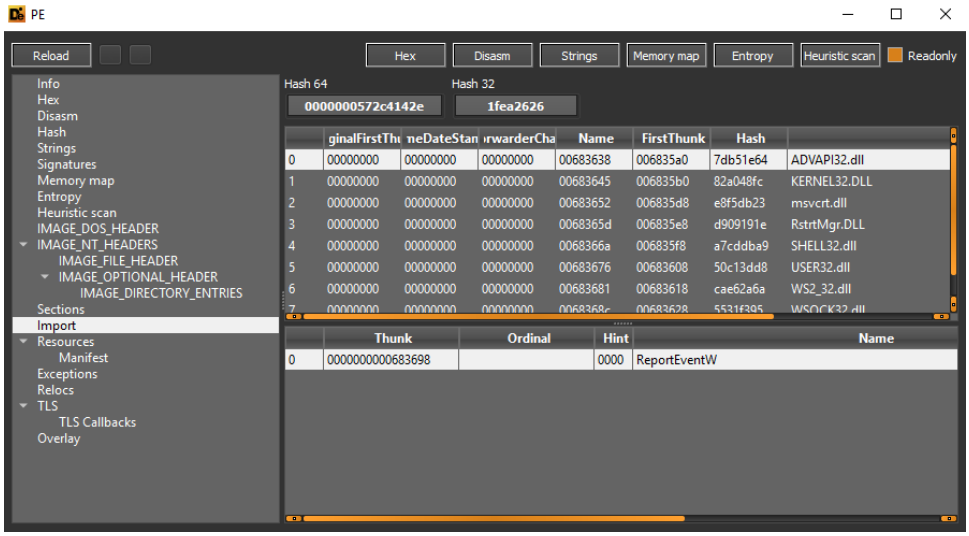


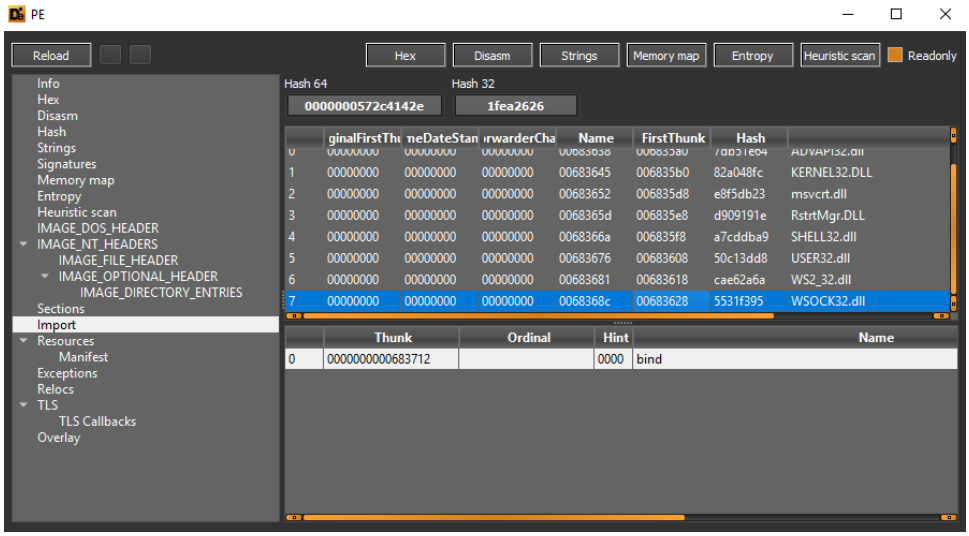


Sempre all'interno dell'Overlay data vi sono dettagli inerenti a quello che sembrerebbe essere un attributo booleano di controllo in merito ad un contesto di leaking.

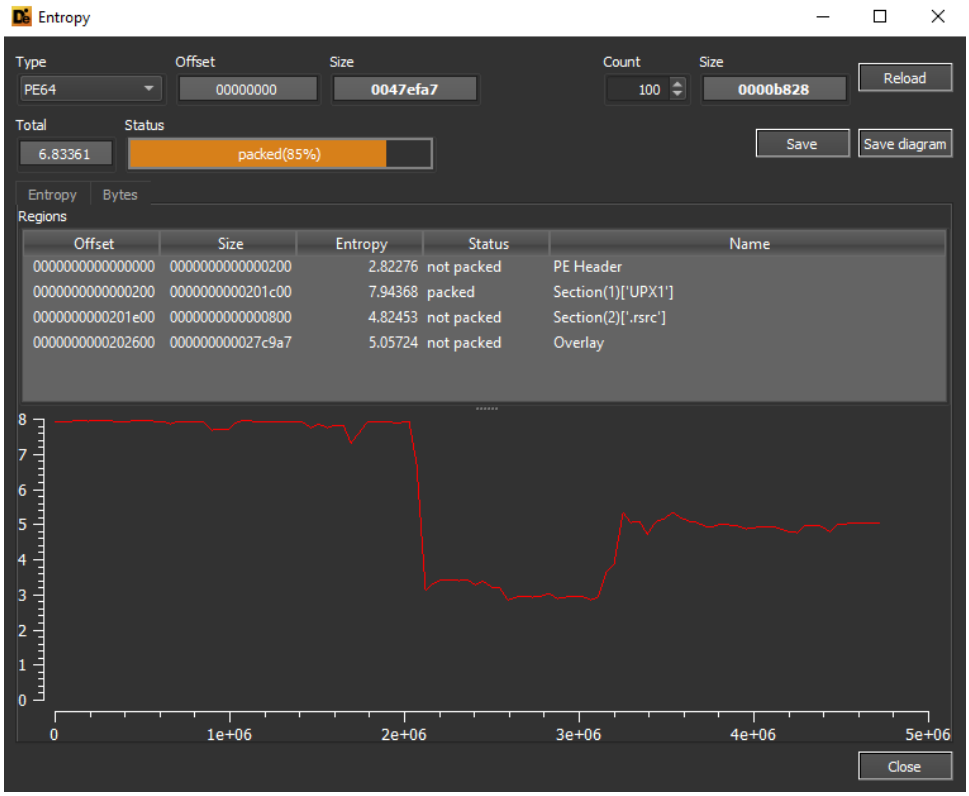


Relativamente agli imports, possiamo evidenziare la libreria *ADVAPI32.dll* (per eseguire la funzione di event log appending *ReportEventW*), *RstrtMgr.dll* (per eseguire la funzione *RmGetList* per ottenere una lista delle applicazioni e dei servizi che utilizzano le risorse registrate all'interno della sessione di Restart Manager), *WS2_32.dll* e *WSOCK32.dll* (al fine di gestire connessioni tramite sockets).



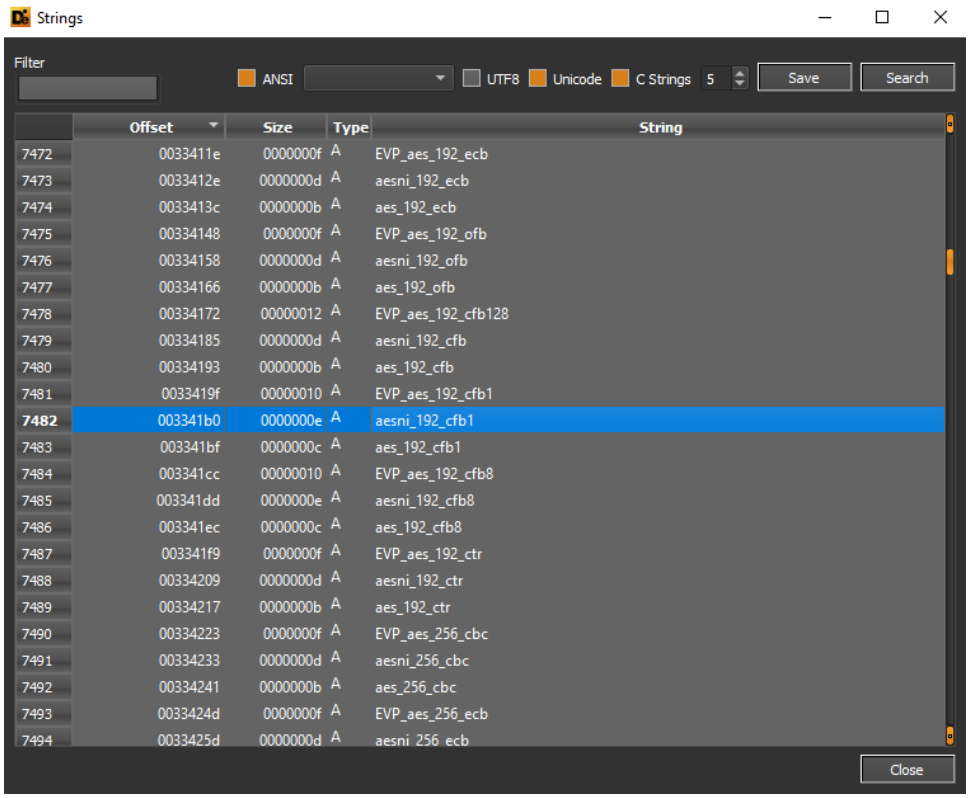


Il coefficiente d'entropia più alto, dovuto alla fase di UPX packing, si attesta a **7.94368**.

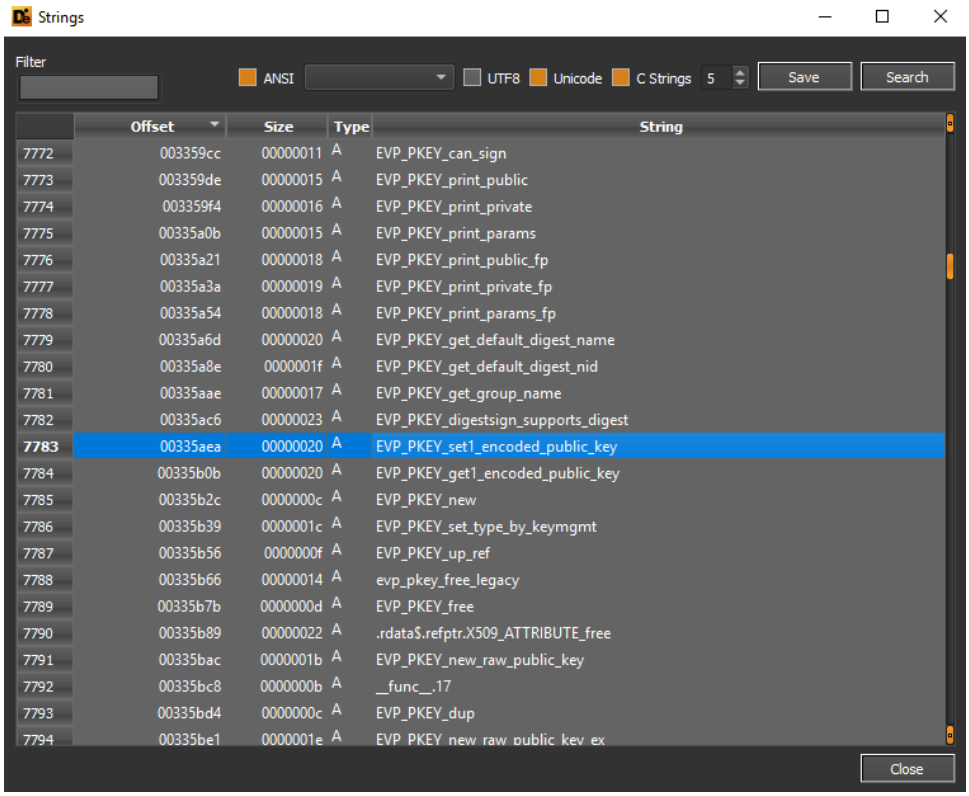



```
File name: C:/Users/IEUser/Desktop/sample/b4kr-xr7h-qcps-omu3.exe
Size: 4714407(4.50 MB)
MD5: e28db6a65da2ebcf304873c9a5ed086d
SHA1: cb570234349507a204c558fc8c4ecf713e2c0ac3
Entropy: 6.83361(packed)
Operation system: Windows(Server 2003)
Architecture: AMD64
Mode: 64-bit
Type: Console
Endianess: LE
Entry point(Address): 00000001406827a0
Entry point(Offset): 002019a0
Entry point(Relative address): 006827a0
Entry point(Bytes): 53565755488d357ae8dfff488dbedbffb7ff488d871c4f5600ff30c700eabaa2cd50
Entry point(Signature): 53565755488d35........488dbe........488d87........ff30c700........50
Entry point(Signature)(Rel): 53565755488d35........488dbe........488d87........ff30c700........50
```

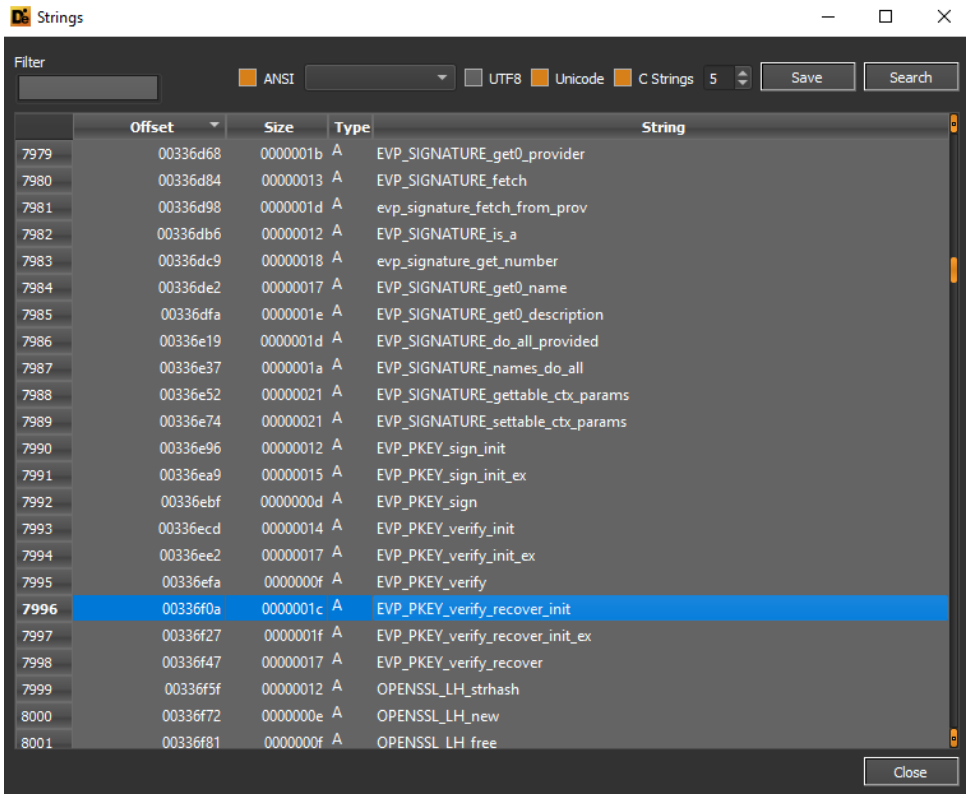
Dalle stringhe estraibili dall'eseguibile si notano riferimenti a *CBC* encryption routines e *CBC* decryption routines relativi all'algoritmo *AES*.



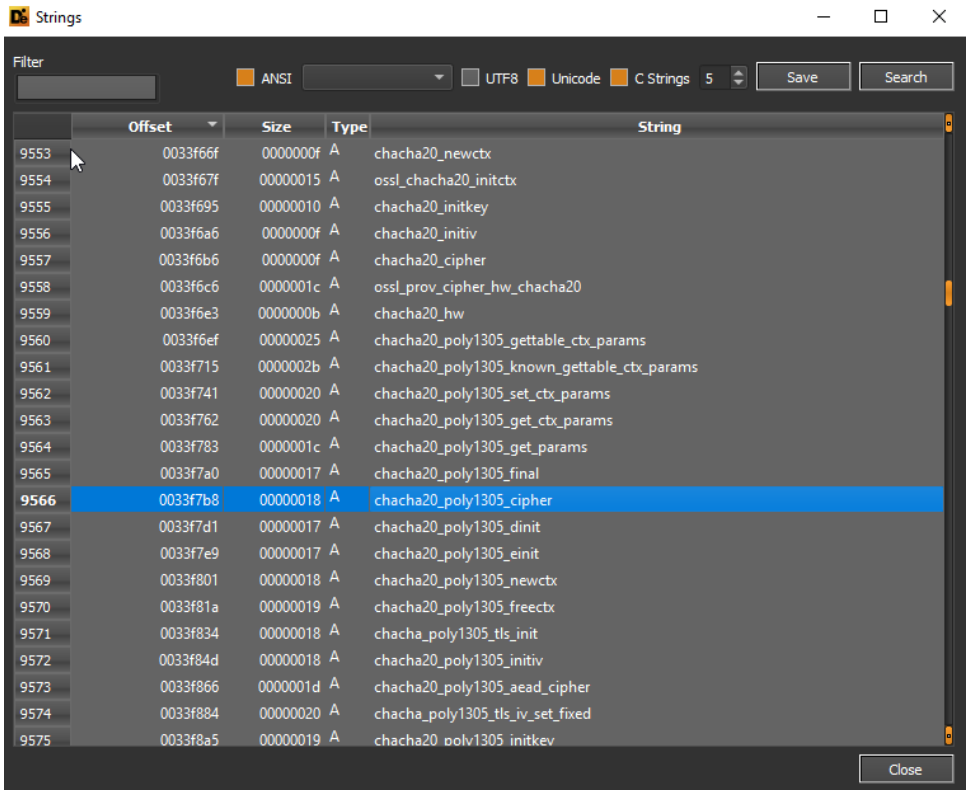
Di seguito i dettagli di alcuni oggetti di public key storage, per esempio *EVP_PKEY_set1_encoded_public_key*:

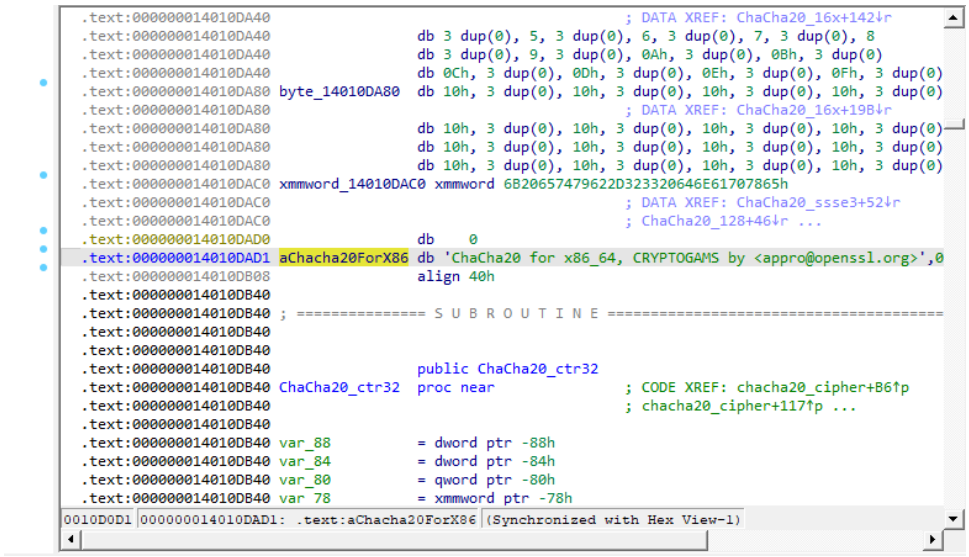


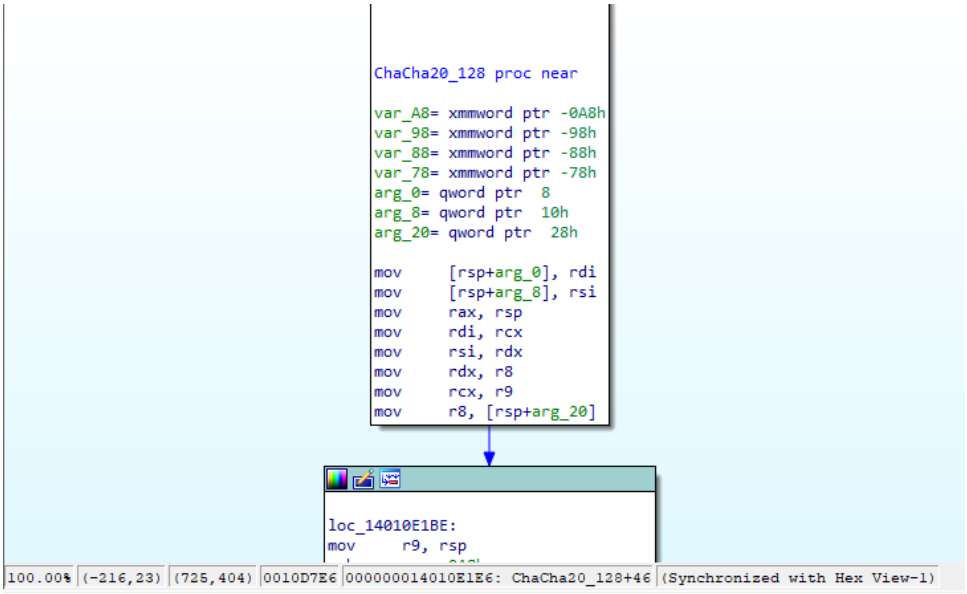
La funzione *EVP_PKEY_verify_recover_init* può essere utilizzata al fine di verificare la signature associata all'algoritmo per la chiave pubblica.



A seguire un dettaglio relativo all' algoritmo *chacha20_poly1305*, viene evidenziato qui sotto l'oggetto cipher. L'algoritmo in questione è un mix tra *ChaCha20* e *Poly1305* e prevede un processo preliminare di authentication.


Strings
Filter
ANSI
UTF8
Unicode
C Strings
5
Save
Search
Offset
Size
Type
String
9553 0033f66f 0000000f A chacha20_newctx
9554 0033f67f 00000015 A ossl_chacha20_initctx
9555 0033f695 00000010 A chacha20_initkey
9556 0033f6a6 0000000f A chacha20_initiv
9557 0033f6b6 0000000f A chacha20_cipher
9558 0033f6c6 0000001c A ossl_prov_cipher_hw_chacha20
9559 0033f6e3 0000000b A chacha20_hw
9560 0033f6ef 00000025 A chacha20_poly1305_gettable_ctx_params
9561 0033f715 0000002b A chacha20_poly1305_known_gettable_ctx_params
9562 0033f741 00000020 A chacha20_poly1305_set_ctx_params
9563 0033f762 00000020 A chacha20_poly1305_get_ctx_params
9564 0033f783 0000001c A chacha20_poly1305_get_params
9565 0033f7a0 00000017 A chacha20_poly1305_final
9566 0033f7b8 00000018 A chacha20_poly1305_cipher
9567 0033f7d1 00000017 A chacha20_poly1305_dinit
9568 0033f7e9 00000017 A chacha20_poly1305_einit
9569 0033f801 00000018 A chacha20_poly1305_newctx
9570 0033f81a 00000019 A chacha20_poly1305_freectx
9571 0033f834 00000018 A chacha_poly1305_tls_init
9572 0033f84d 00000018 A chacha20_poly1305_initiv
9573 0033f866 0000001d A chacha20_poly1305_aead_cipher
9574 0033f884 00000020 A chacha_poly1305_tls_iv_set_fixed
9575 0033f8a5 00000019 A chacha20_poly1305_initkey
Close


.text:000000014010DA40 ; DATA XREF: ChaCha20_16x+142↓r
.text:000000014010DA40 db 3 dup(0), 5, 3 dup(0), 6, 3 dup(0), 7, 3 dup(0), 8
.text:000000014010DA40 db 3 dup(0), 9, 3 dup(0), 0Ah, 3 dup(0), 0Bh, 3 dup(0)
.text:000000014010DA40 db 0Ch, 3 dup(0), 0Dh, 3 dup(0), 0Eh, 3 dup(0), 0Fh, 3 dup(0)
.text:000000014010DA80 byte_14010DA80 db 10h, 3 dup(0), 10h, 3 dup(0), 10h, 3 dup(0), 10h, 3 dup(0)
.text:000000014010DA80 ; DATA XREF: ChaCha20_16x+19B↓r
.text:000000014010DA80 db 10h, 3 dup(0), 10h, 3 dup(0), 10h, 3 dup(0), 10h, 3 dup(0)
.text:000000014010DA80 db 10h, 3 dup(0), 10h, 3 dup(0), 10h, 3 dup(0), 10h, 3 dup(0)
.text:000000014010DA80 db 10h, 3 dup(0), 10h, 3 dup(0), 10h, 3 dup(0), 10h, 3 dup(0)
.text:000000014010DAC0 xmmword_14010DAC0 xmmword 6B20657479622D323320646E61707865h
.text:000000014010DAC0 ; DATA XREF: ChaCha20_ssse3+52↓r
.text:000000014010DAC0 ; ChaCha20_128+46↓r ...
.text:000000014010DAD0 db 0
.text:000000014010DAD1 aChacha20ForX86 db 'ChaCha20 for x86_64, CRYPTOGAMS by <appro@openssl.org>',0
.text:000000014010DB08 align 40h
.text:000000014010DB40
.text:000000014010DB40 ; =============== S U B R O U T I N E =======================================
.text:000000014010DB40
.text:000000014010DB40
.text:000000014010DB40 public ChaCha20_ctr32
.text:000000014010DB40 ChaCha20_ctr32 proc near ; CODE XREF: chacha20_cipher+B6↑p
.text:000000014010DB40 ; chacha20_cipher+117↑p ...
.text:000000014010DB40
.text:000000014010DB40 var_88 = dword ptr -88h
.text:000000014010DB40 var_84 = dword ptr -84h
.text:000000014010DB40 var_80 = qword ptr -80h
.text:000000014010DB40 var_78 = xmmword ptr -78h
0010D0D1 000000014010DAD1: .text:aChacha20ForX86 (Synchronized with Hex View-1)



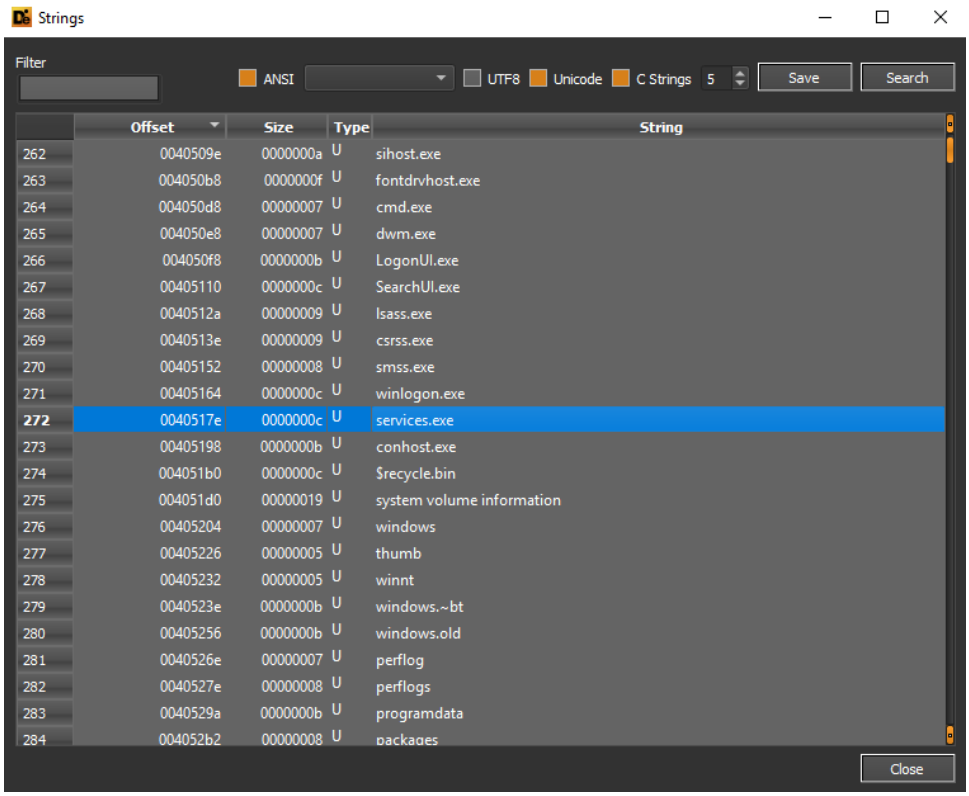
Nello screenshot sottostante sono invece evidenziate funzioni di loading della chiave privata associata a *OpenSSL*:

	Offset	Size	Type	String
13120	00353357	0000001d	A	ossl_ecx_key_allocate_privkey
13377	00354b1a	00000014	A	openssl_load_privkey
13392	00354c0b	00000020	A	ENGINE_set_load_privkey_function
13395	00354c75	00000020	A	ENGINE_get_load_privkey_function

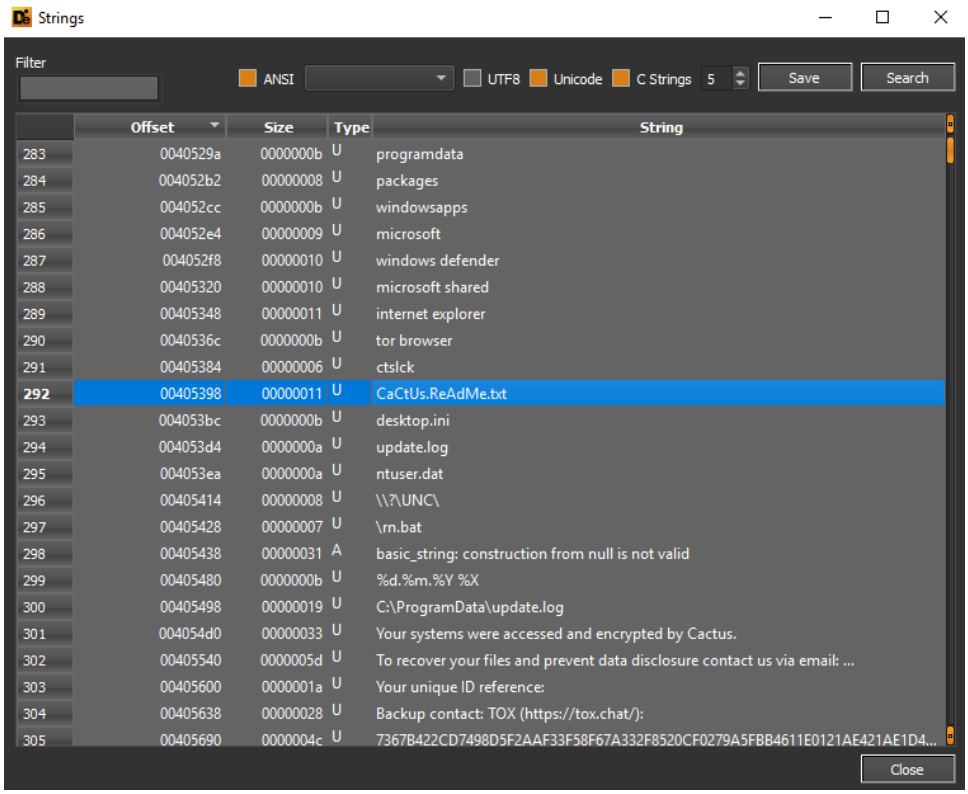
Qui di seguito la fase di unpacking UPX:

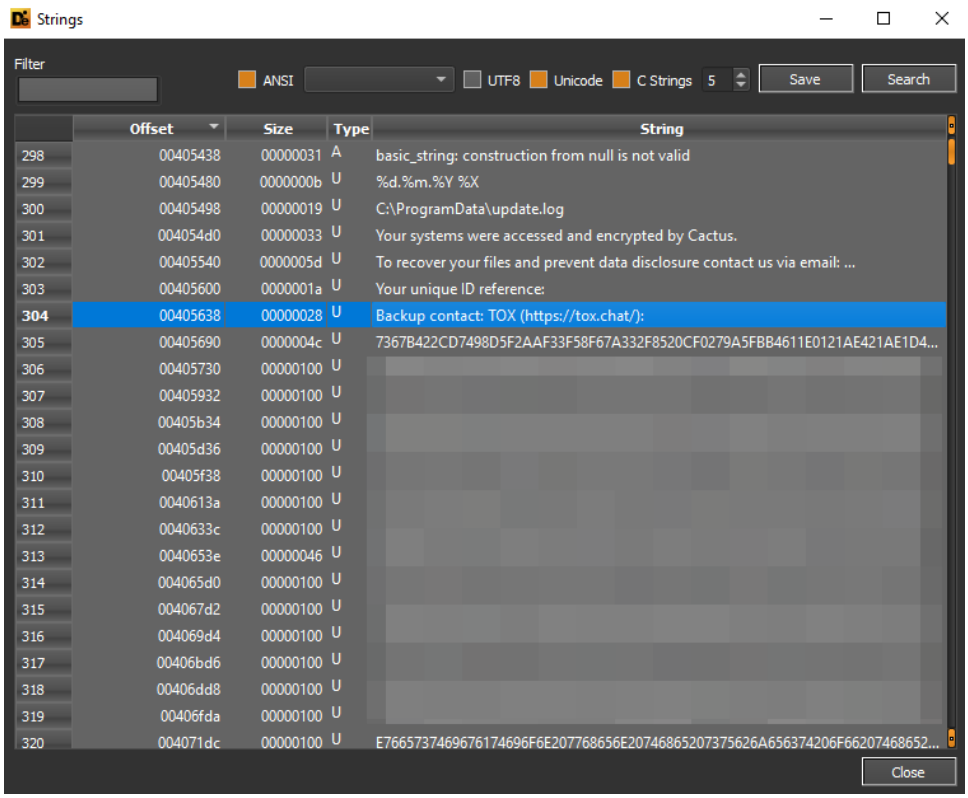
```
C:\Windows\system32>C:\Users\IEUser\Desktop\upx-4.0.2-win64\upx.exe -d C:\Users\IEUser\Desktop\sample\b4kr-xr7h-qcps-omu
3.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2023
UPX 4.0.2       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 30th 2023

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
   9088423 <-   4714407   51.87%    win64/pe     b4kr-xr7h-qcps-omu3.exe

Unpacked 1 file.

C:\Windows\system32>
```

Dalle stringhe estratte vi sono dettagli inerenti a processi di authentication (*lsass.exe* e *winlogon.exe*), *services.exe*, la cartella *ProgramData*.

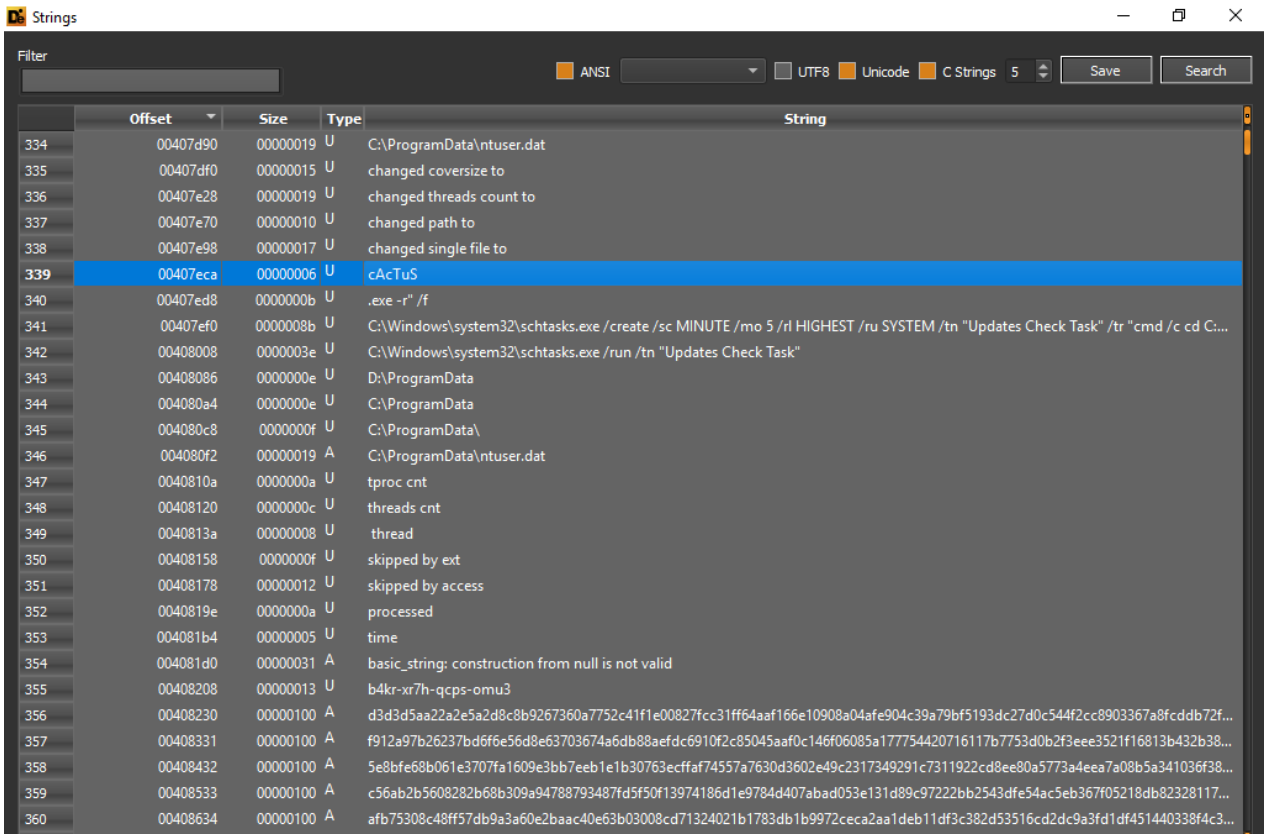


Cactus Ransomware effettua il bypassing della protection di Windows Defender, utilizza TOR Browser per il contatto con i malcoders, il file *ntuser.dat* (salvato nella cartella C:\ProgramData) viene utilizzato con lo scopo di archiviare la chiave per la crittografia del file eseguibile. Esso non rappresenta il file ntuser.dat originale di Windows ma piuttosto un file denominato in tal modo con tutta probabilità per effettuare evasion e confondere la natura del file stesso. Inoltre, lo script batch *rn.bat* viene con tutta probabilità utilizzato per la fase di rinomina di files. Il file di log *C:\ProgramData\update.log* viene utilizzato per tracciamento dell'infezione ransomware, mentre il threat minaccia anche la pubblicazione dei dati della vittima in caso di mancato pagamento del riscatto.


Strings
Filter
ANSI
UTF8
Unicode
C Strings
5
Save
Search
Offset
Size
Type
String
283 0040529a 0000000b U programdata
284 004052b2 00000008 U packages
285 004052cc 0000000b U windowsapps
286 004052e4 00000009 U microsoft
287 004052f8 00000010 U windows defender
288 00405320 00000010 U microsoft shared
289 00405348 00000011 U internet explorer
290 0040536c 0000000b U tor browser
291 00405384 00000006 U ctslck
292 00405398 00000011 U CaCtUs.ReAdMe.txt
293 004053bc 0000000b U desktop.ini
294 004053d4 0000000a U update.log
295 004053ea 0000000a U ntuser.dat
296 00405414 00000008 U \\?\UNC\
297 00405428 00000007 U \rn.bat
298 00405438 00000031 A basic_string: construction from null is not valid
299 00405480 0000000b U %d.%m.%Y %X
300 00405498 00000019 U C:\ProgramData\update.log
301 004054d0 00000033 U Your systems were accessed and encrypted by Cactus.
302 00405540 0000005d U To recover your files and prevent data disclosure contact us via email: ...
303 00405600 0000001a U Your unique ID reference:
304 00405638 00000028 U Backup contact: TOX (https://tox.chat/):
305 00405690 0000004c U 7367B422CD7498D5F2AAF33F58F67A332F8520CF0279A5FBB4611E0121AE421AE1D4...
Close

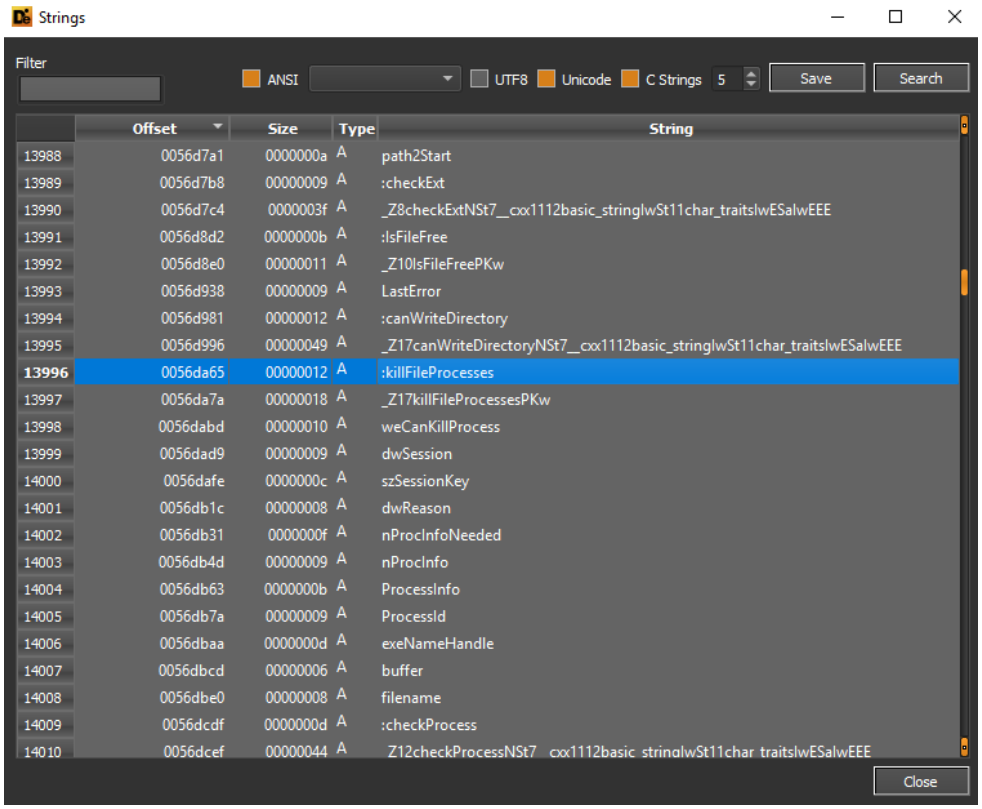

Strings
Filter
ANSI
UTF8
Unicode
C Strings
5
Save
Search
Offset
Size
Type
String
298 00405438 00000031 A basic_string: construction from null is not valid
299 00405480 0000000b U %d.%m.%Y %X
300 00405498 00000019 U C:\ProgramData\update.log
301 004054d0 00000033 U Your systems were accessed and encrypted by Cactus.
302 00405540 0000005d U To recover your files and prevent data disclosure contact us via email: ...
303 00405600 0000001a U Your unique ID reference:
304 00405638 00000028 U Backup contact: TOX (https://tox.chat/):
305 00405690 0000004c U 7367B422CD7498D5F2AAF33F58F67A332F8520CF0279A5FBB4611E0121AE421AE1D4...
306 00405730 00000100 U
307 00405932 00000100 U
308 00405b34 00000100 U
309 00405d36 00000100 U
310 00405f38 00000100 U
311 0040613a 00000100 U
312 0040633c 00000100 U
313 0040653e 00000046 U
314 004065d0 00000100 U
315 004067d2 00000100 U
316 004069d4 00000100 U
317 00406bd6 00000100 U
318 00406dd8 00000100 U
319 00406fda 00000100 U
320 004071dc 00000100 U E76657374696761746 96F6E207768656E2074686520737562A656374206F66207468652...
Close

Cactus Ransomware crea uno scheduled task per la persistenza malevola denominato ***"Updates Check Task"***



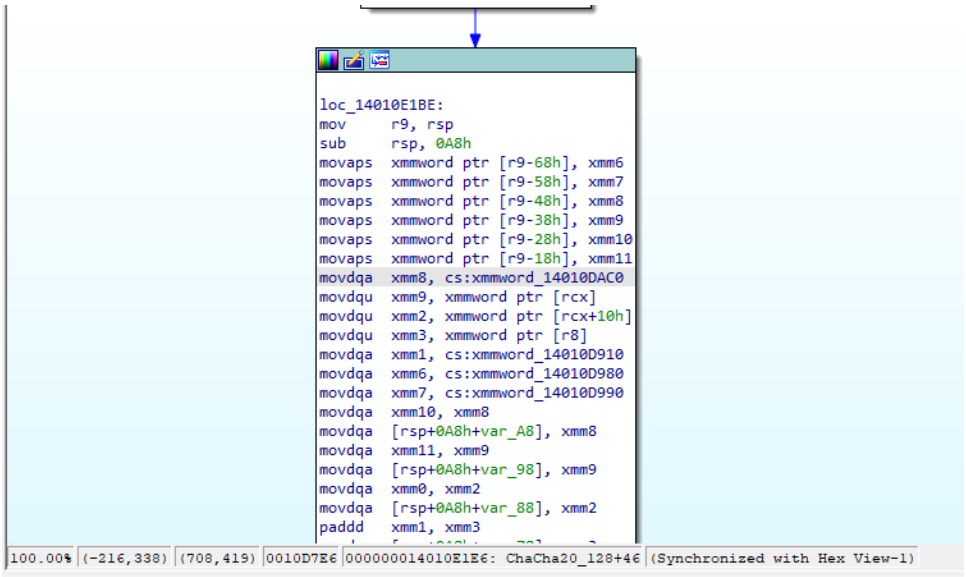
	Offset	Size	Type	String
334	00407d90	00000019	U	C:\ProgramData\ntuser.dat
335	00407df0	00000015	U	changed coversize to
336	00407e28	00000019	U	changed threads count to
337	00407e70	00000010	U	changed path to
338	00407e98	00000017	U	changed single file to
339	00407eca	00000006	U	cAcTuS
340	00407ed8	0000000b	U	.exe -r" /f
341	00407ef0	0000008b	U	C:\Windows\system32\schtasks.exe /create /sc MINUTE /mo 5 /rl HIGHEST /ru SYSTEM /tn "Updates Check Task" /tr "cmd /c cd C:...
342	00408008	0000003e	U	C:\Windows\system32\schtasks.exe /run /tn "Updates Check Task"
343	00408086	0000000e	U	D:\ProgramData
344	004080a4	0000000e	U	C:\ProgramData
345	004080c8	0000000f	U	C:\ProgramData\
346	004080f2	00000019	A	C:\ProgramData\ntuser.dat
347	0040810a	0000000a	U	tproc cnt
348	00408120	0000000c	U	threads cnt
349	0040813a	00000008	U	thread
350	00408158	0000000f	U	skipped by ext
351	00408178	00000012	U	skipped by access
352	0040819e	0000000a	U	processed
353	004081b4	00000005	U	time
354	004081d0	00000031	A	basic_string: construction from null is not valid
355	00408208	00000013	U	b4kr-xr7h-qcps-omu3
356	00408230	00000100	A	d3d3d5aa22a2e5a2d8c8b9267360a7752c41f1e00827fcc31ff64aaf166e10908a04afe904c39a79bf5193dc27d0c544f2cc8903367a8fcddb72f...
357	00408331	00000100	A	f912a97b26237bd6f6e56d8e63703674a6db88aefdc6910f2c85045aaf0c146f06085a177754420716117b7753d0b2f3eee3521f16813b432b38...
358	00408432	00000100	A	5e8bfe68b061e3707fa1609e3bb7eeb1e1b30763ecffaf74557a7630d3602e49c2317349291c7311922cd8ee80a5773a4eea7a08b5a341036f38...
359	00408533	00000100	A	c56ab2b5608282b68b309a94788793487fd5f50f13974186d1e9784d407abad053e131d89c97222bb2543dfe54ac5eb367f05218db82328117...
360	00408634	00000100	A	afb75308c48ff57db9a3a60e2baac40e63b03008cd71324021b1783db1b9972ceca2aa1deb11df3c382d53516cd2dc9a3fd1df451440338f4c3...

Si notino le funzioni *IsFileFree* (che viene utilizzata al fine di controllare se un determinato file si può criptare), *canWriteDirectory* (per controllare se una determinata cartella permette eventi di scrittura), *killFileProcesses* (con lo scopo di terminare i processi che occupano le risorse di un determinato file), *weCanKillProcess* (utilizzabile al fine di controllare se un determinato processo può essere terminato)



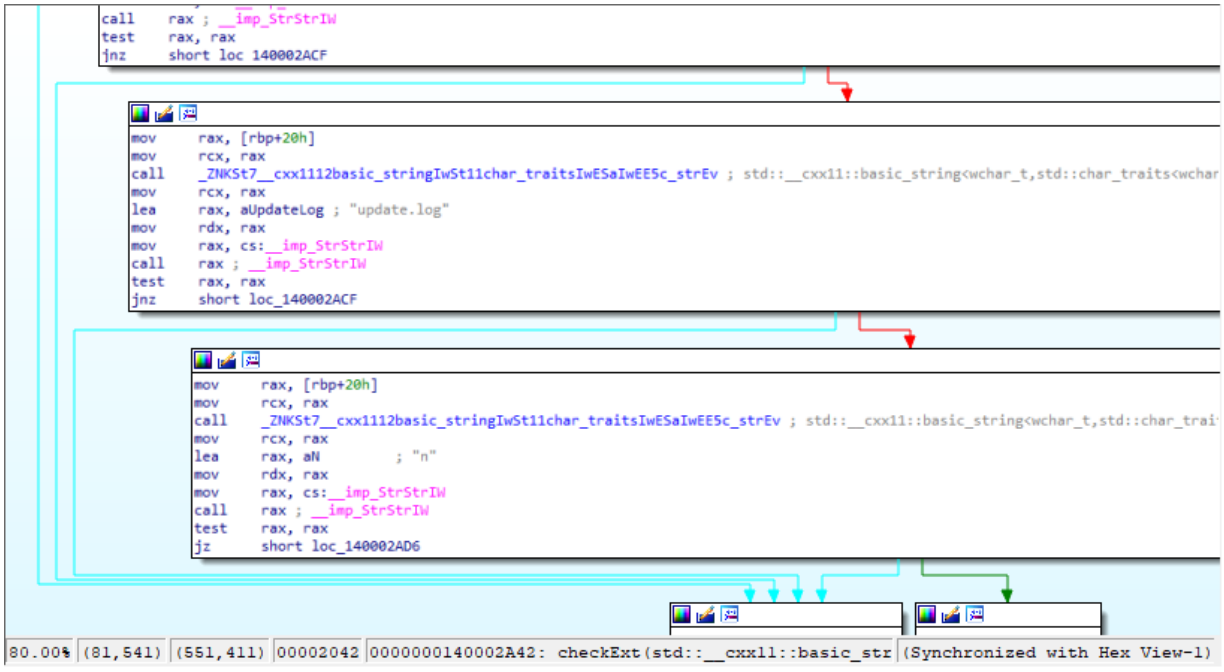
Analisi dinamica e disassembling

Contestualmente ad esecuzioni ChaCha20, all'interno della label *loc_14010E1BE*, vi sono numerose operazioni *movaps, movdqa* e *movdqu* inerenti a registri *xmm*



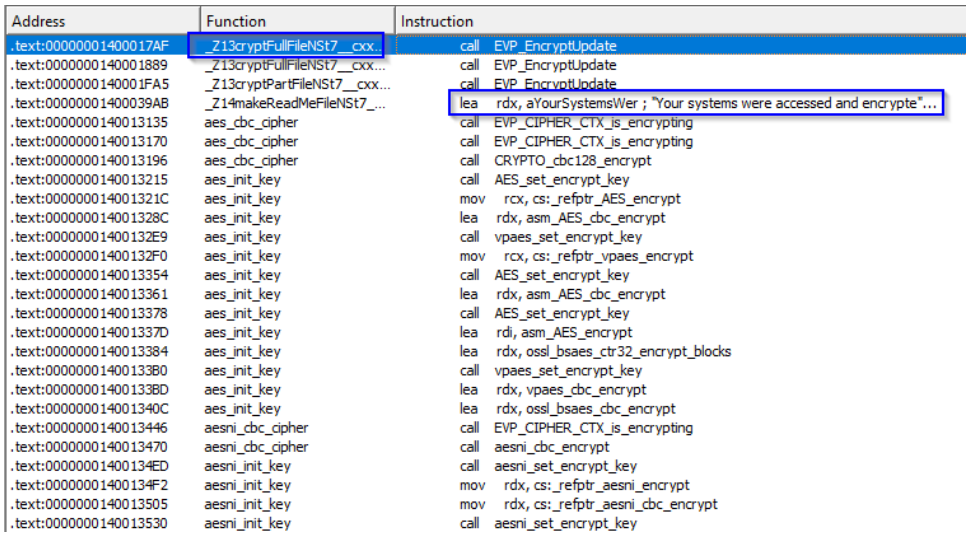
Cactus Ransomware effettua modifiche in merito al file di configurazione *desktop.ini* conseguentemente alla fase di desktop changing e readme notes dropping, per quanto riguarda il file di tracciamento *update.log* vengono anche aggiunti attributi di newline:


var_18= byte ptr -18h
push rbp
push rbx
sub rsp, 58h
lea rbp, [rsp+68h+var_18]
mov [rbp+20h], rcx
mov rax, [rbp+20h]
mov rcx, rax
call _ZNKSt7__cxx1112basic_stringIwSt11char_traitsIwESaIwEE5c_strEv ; std::__cxx11::basic_string<wchar_t,std::char_traits<wchar_t>,std::a
mov rcx, rax
lea rax, aCactusReadmeTx ; "CaCtUs.ReAdMe.txt"
mov rdx, rax
mov rax, cs:__imp_StrStrIW
call rax ; __imp_StrStrIW
test rax, rax
jnz short loc 140002ACF
mov rax, [rbp+20h]
mov rcx, rax
call _ZNKSt7__cxx1112basic_stringIwSt11char_traitsIwESaIwEE5c_strEv ; std::__cxx11::basic_string<wchar_t,std::char_traits<wchar_t>,std:
mov rcx, rax
lea rax, aDesktopIni ; "desktop.ini"
mov rdx, rax
mov rax, cs:__imp_StrStrIW
call rax ; __imp_StrStrIW
test rax, rax
jnz short loc_140002ACF
80.00% (113,128) (601,414) 00002042 0000000140002A42: checkExt(std::__cxx11::basic_st (Synchronized with Hex View-1)


call rax ; __imp_StrStrIW
test rax, rax
jnz short loc 140002ACF
mov rax, [rbp+20h]
mov rcx, rax
call _ZNKSt7__cxx1112basic_stringIwSt11char_traitsIwESaIwEE5c_strEv ; std::__cxx11::basic_string<wchar_t,std::char_traits<wchar
mov rcx, rax
lea rax, aUpdateLog ; "update.log"
mov rdx, rax
mov rax, cs:__imp_StrStrIW
call rax ; __imp_StrStrIW
test rax, rax
jnz short loc_140002ACF
mov rax, [rbp+20h]
mov rcx, rax
call _ZNKSt7__cxx1112basic_stringIwSt11char_traitsIwESaIwEE5c_strEv ; std::__cxx11::basic_string<wchar_t,std::char_trai
mov rcx, rax
lea rax, aN ; "n"
mov rdx, rax
mov rax, cs:__imp_StrStrIW
call rax ; __imp_StrStrIW
test rax, rax
jz short loc_140002AD6
80.00% (81,541) (551,411) 00002042 0000000140002A42: checkExt(std::__cxx11::basic_str (Synchronized with Hex View-1)

L'indirizzo e-mail **cactus[@]mexicomail[.]com** è l'indirizzo di contatto dei malcoders:

Qui una stringa di introduzione del file di readme del ransomware:

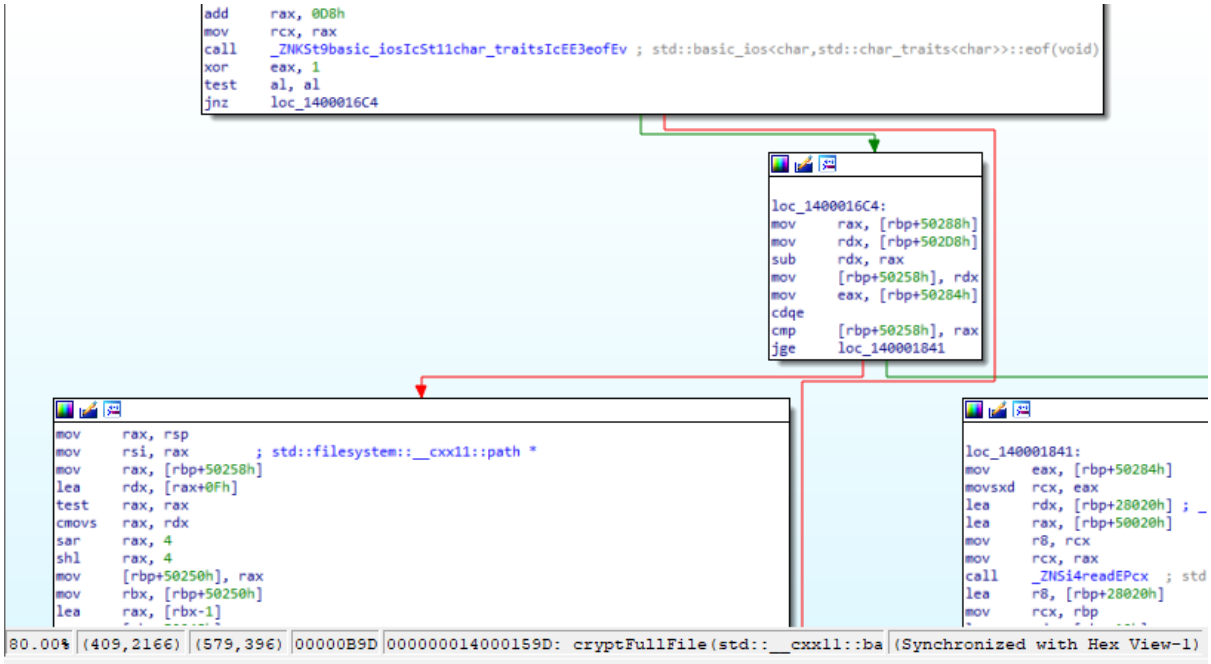


All'interno della funzione *cryptFullFile* è stata richiamata la funzione *EVP_EncryptUpdate* e funzioni di *istream* e *ostream* per la gestione degli attributi dei files presi in considerazione durante la fase di encryption:

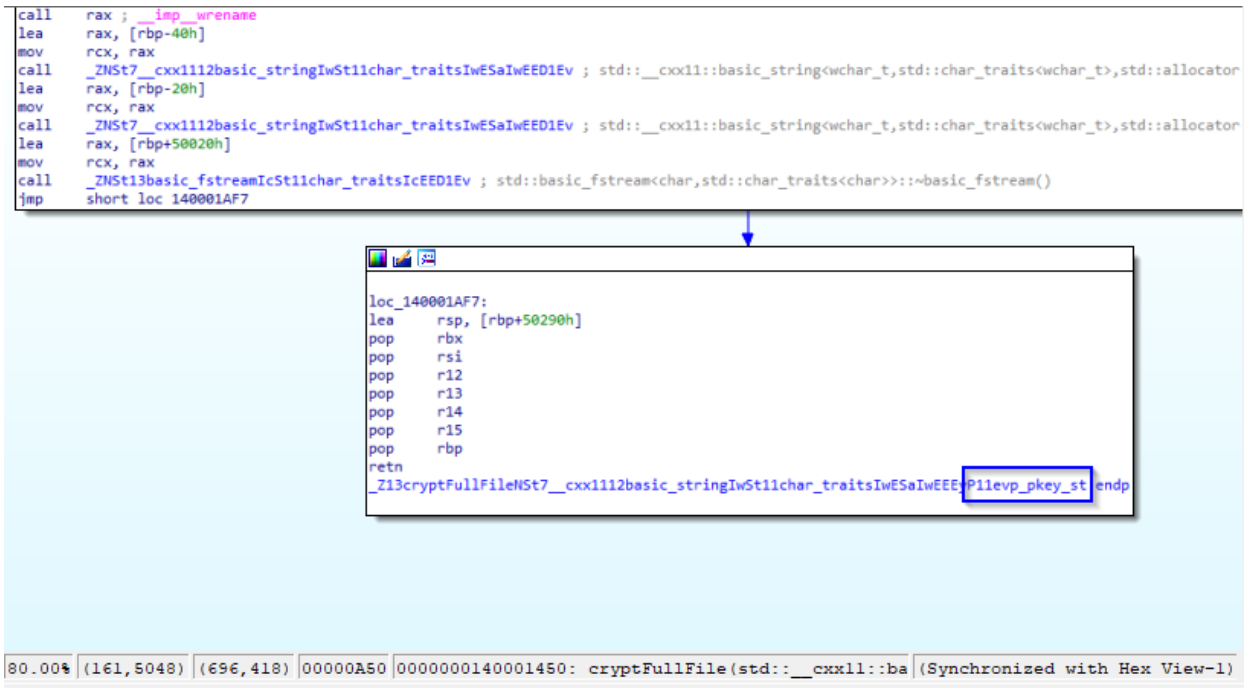
Inizialmente viene “appesa” l’estensione *“.cts0”* ai files criptati:

Successivamente viene sostituita con l'estensione *".cts1"*:

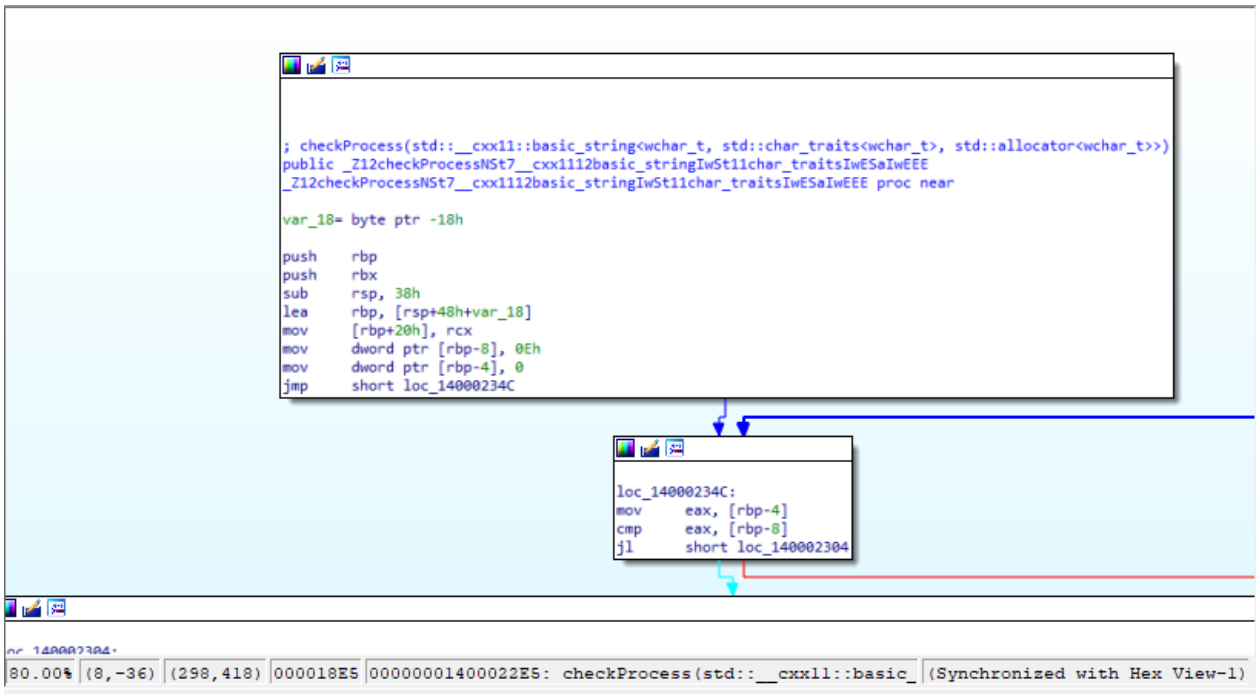
Vi è l'utilizzo della wildcard "*" per la gestione di filesystem enumeration:



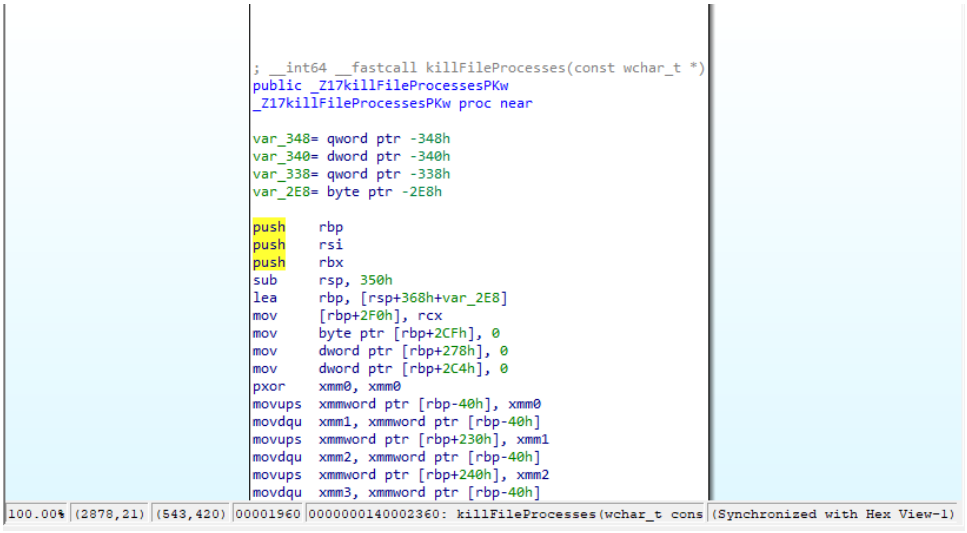
A seguire un riferimento ad un oggetto di encryption key contestualmente al richiamo della funzione cryptFullFile:

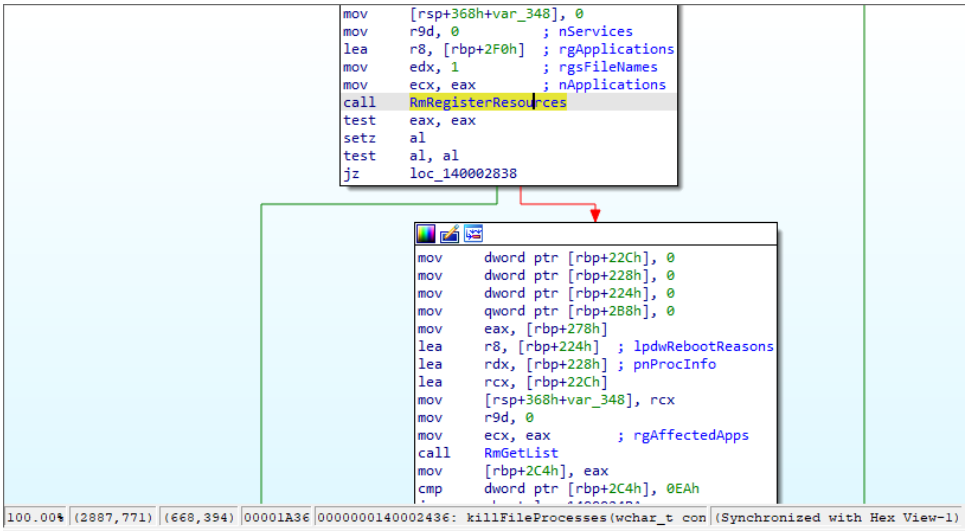


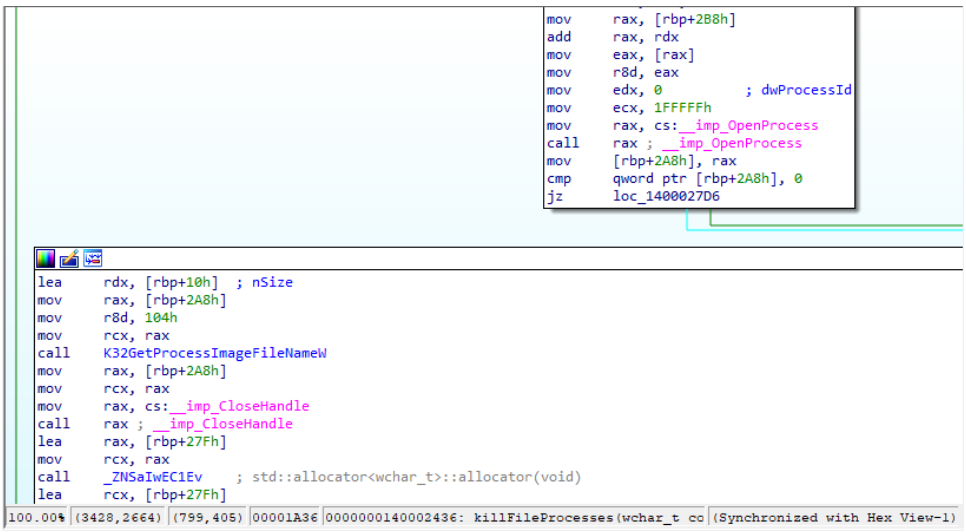
Qui la funzione di enumerazione dei dischi della macchina compromessa:



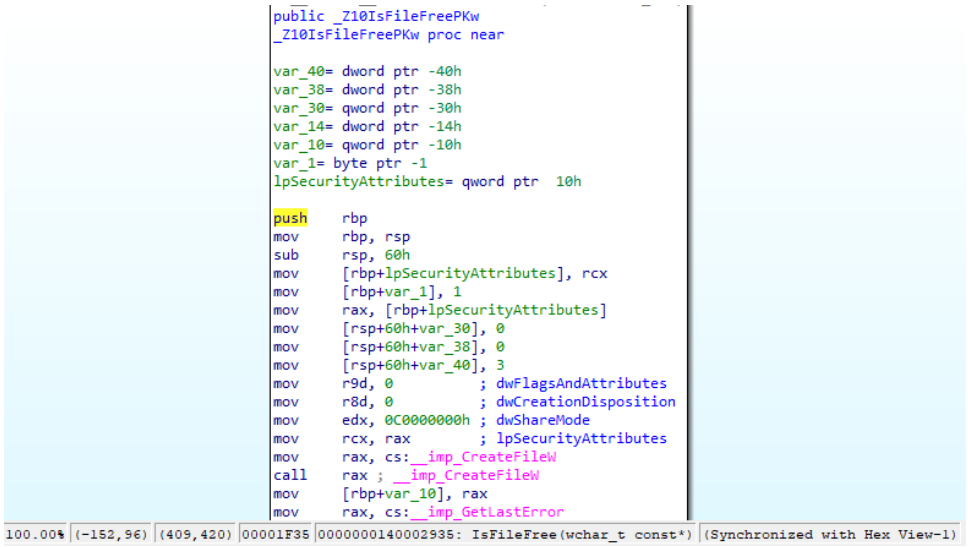
A seguire i dettagli della funzione *killFileProcesses* che include la gestione del *RestartManager* per "liberare" le risorse dei files da criptare dai processi che li stanno (eventualmente) utilizzando.

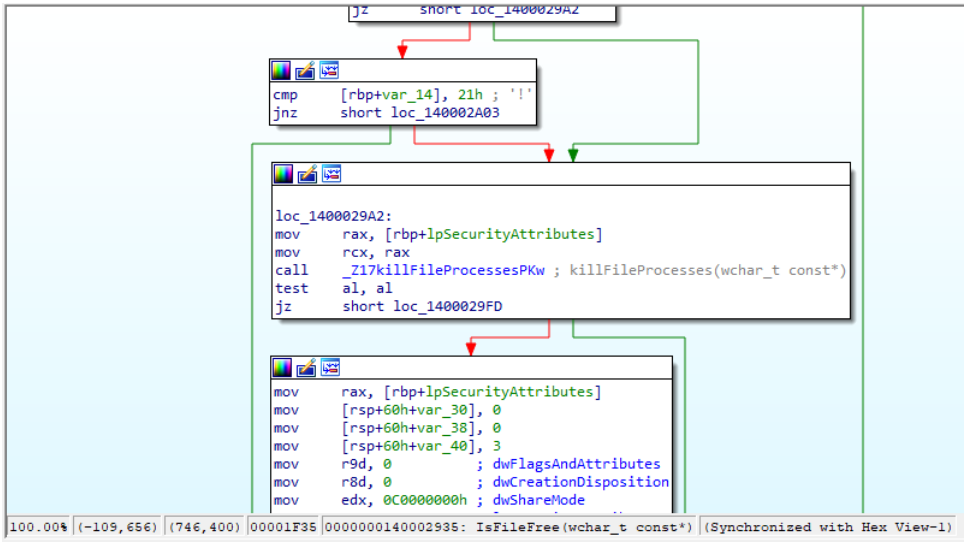

; __int64 __fastcall killFileProcesses(const wchar_t *)
public _Z17killFileProcessesPKw
_Z17killFileProcessesPKw proc near
var_348= qword ptr -348h
var_340= dword ptr -340h
var_338= qword ptr -338h
var_2E8= byte ptr -2E8h
push rbp
push rsi
push rbx
sub rsp, 350h
lea rbp, [rsp+368h+var_2E8]
mov [rbp+2F0h], rcx
mov byte ptr [rbp+2CFh], 0
mov dword ptr [rbp+278h], 0
mov dword ptr [rbp+2C4h], 0
pxor xmm0, xmm0
movups xmmword ptr [rbp-40h], xmm0
movdqu xmm1, xmmword ptr [rbp-40h]
movups xmmword ptr [rbp+230h], xmm1
movdqu xmm2, xmmword ptr [rbp-40h]
movups xmmword ptr [rbp+240h], xmm2
movdqu xmm3, xmmword ptr [rbp-40h]
100.00% (2878,21) (543,420) 00001960 0000000140002360: killFileProcesses(wchar_t cons (Synchronized with Hex View-1)


mov [rsp+368h+var_348], 0
mov r9d, 0 ; nServices
lea r8, [rbp+2F0h] ; rgApplications
mov edx, 1 ; rgsFileNames
mov ecx, eax ; nApplications
call RmRegisterResources
test eax, eax
setz al
test al, al
jz loc_140002838
mov dword ptr [rbp+22Ch], 0
mov dword ptr [rbp+228h], 0
mov dword ptr [rbp+224h], 0
mov qword ptr [rbp+2B8h], 0
mov eax, [rbp+278h]
lea r8, [rbp+224h] ; lpdwRebootReasons
lea rdx, [rbp+228h] ; pnProcInfo
lea rcx, [rbp+22Ch]
mov [rsp+368h+var_348], rcx
mov r9d, 0
mov ecx, eax ; rgAffectedApps
call RmGetList
mov [rbp+2C4h], eax
cmp dword ptr [rbp+2C4h], 0EAh
100.00% (2887,771) (668,394) 00001A36 0000000140002436: killFileProcesses(wchar_t con (Synchronized with Hex View-1)


mov rax, [rbp+2B8h]
add rax, rdx
mov eax, [rax]
mov r8d, eax
mov edx, 0 ; dwProcessId
mov ecx, 1FFFFFh
mov rax, cs:__imp_OpenProcess
call rax ; __imp_OpenProcess
mov [rbp+2A8h], rax
cmp qword ptr [rbp+2A8h], 0
jz loc_1400027D6
lea rdx, [rbp+10h] ; nSize
mov rax, [rbp+2A8h]
mov r8d, 104h
mov rcx, rax
call K32GetProcessImageFileNameW
mov rax, [rbp+2A8h]
mov rcx, rax
mov rax, cs:__imp_CloseHandle
call rax ; __imp_CloseHandle
lea rax, [rbp+27Fh]
mov rcx, rax
call _ZNSaIwEC1Ev ; std::allocator<wchar_t>::allocator(void)
lea rcx, [rbp+27Fh]
100.00% (3428,2664) (799,405) 00001A36 0000000140002436: killFileProcesses(wchar_t co (Synchronized with Hex View-1)

Di seguito un riferimento che sembrerebbe essere associato all'accesso a network shares, nonché un accesso concorrenziale ai files da criptare, prendendo in considerazione gli attributi degli stessi ed attraverso una conferma booleana:

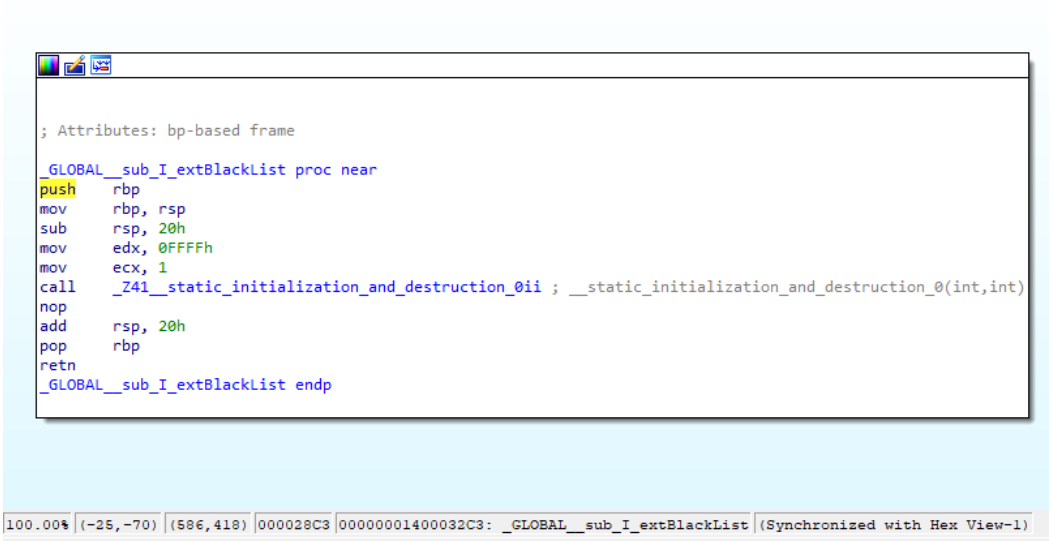




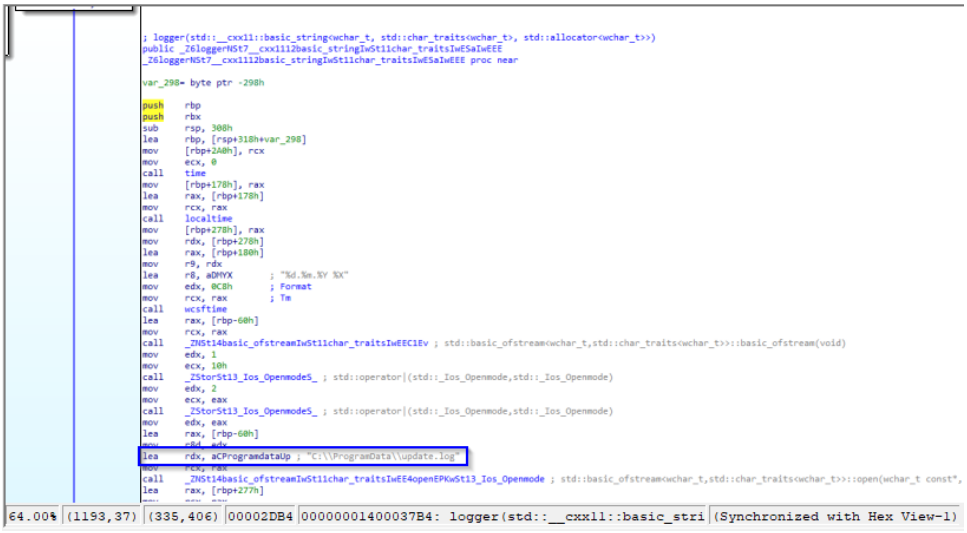
Lo script *rn.bat* viene molto probabilmente utilizzato in fase di rinomina dei files presi in considerazione durante l'infection kill chain:

La funzione *extractDirPath* ottiene i filenames dato un path specifico:

Cactus Ransomware possiede un attributo globale, il quale sembrerebbe far riferimento ad una blacklist di estensioni, difatti denominata *extBlackList*:

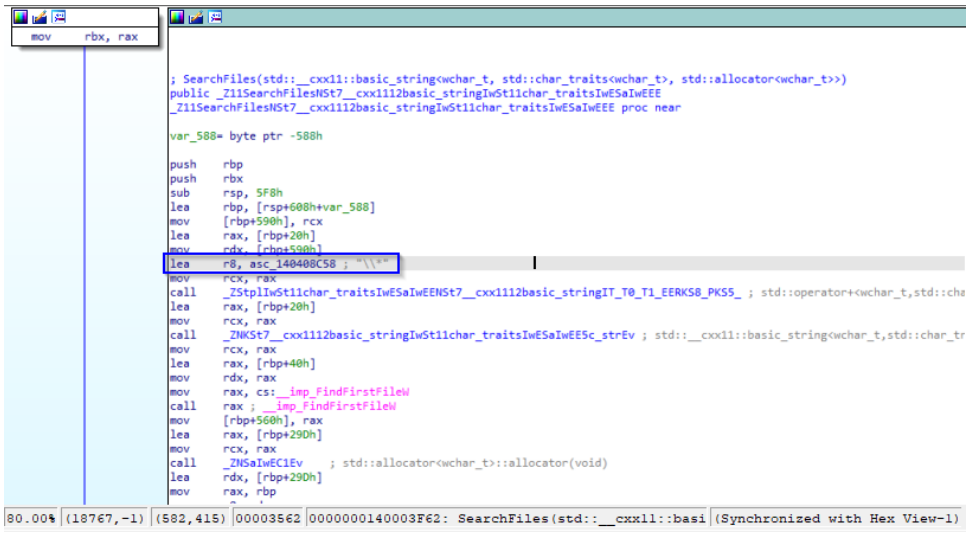


La funzione *hexEncode* prende come parametro in input la variabile *var_178*, utilizzata in un'istruzione *lea* con il registro *rbp*, per caricare l'indirizzo di memoria in questione:

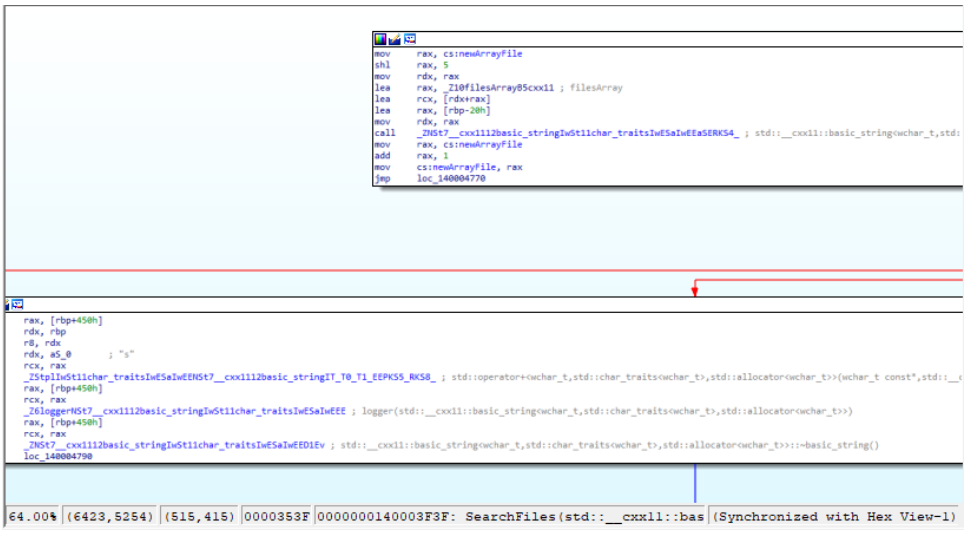


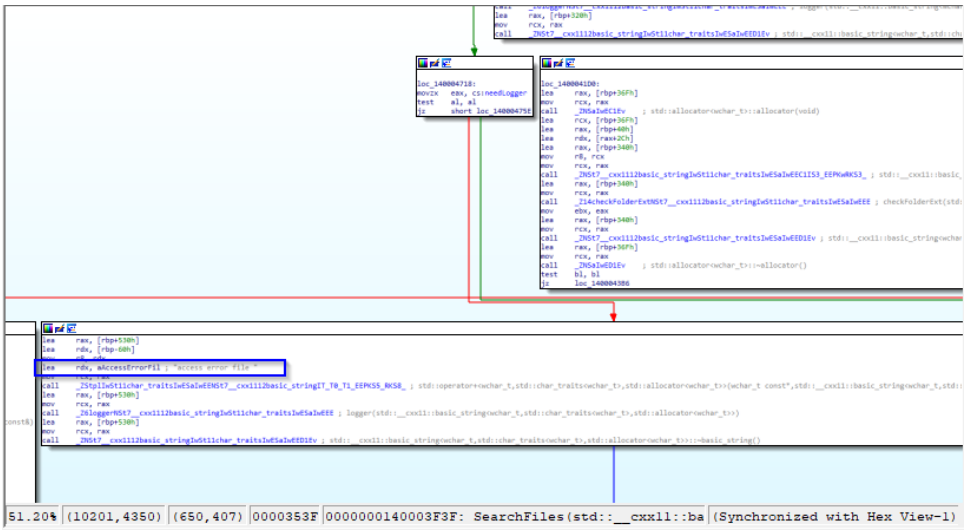
La funzione *makeNtUserFile* risulta essere fondamentale al fine di salvare la stringa di crittografia del ransomware stesso in fase di post-infection-deployment:

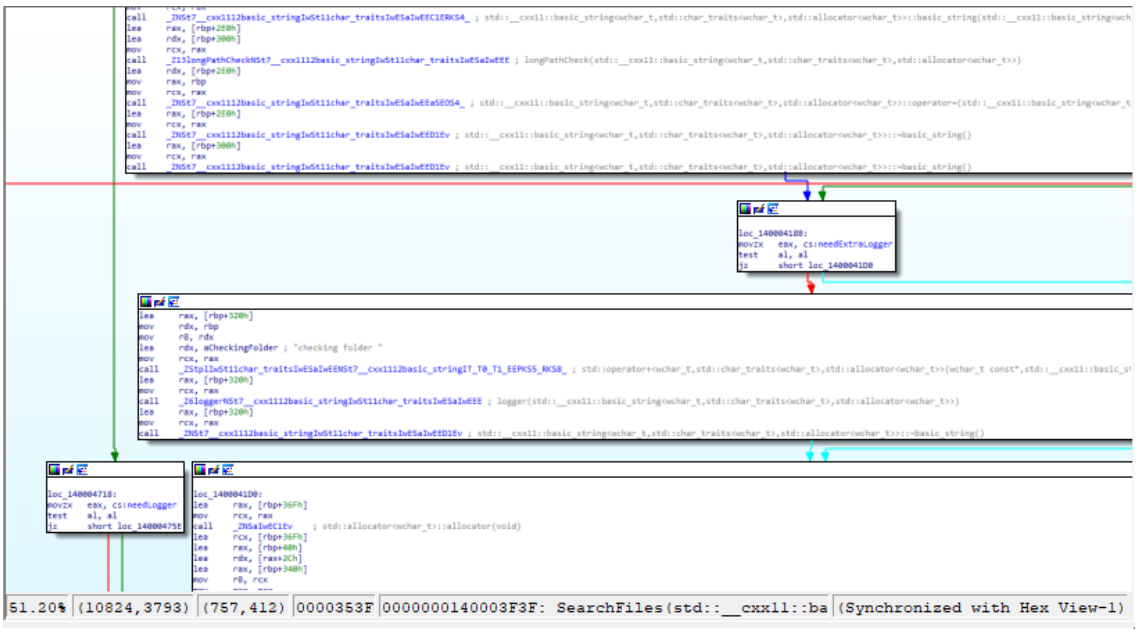
Qui la wildcard "*", utilizzata in fase di files enumeration loop per ottenere i files da sottoporre al processo di crittografia:



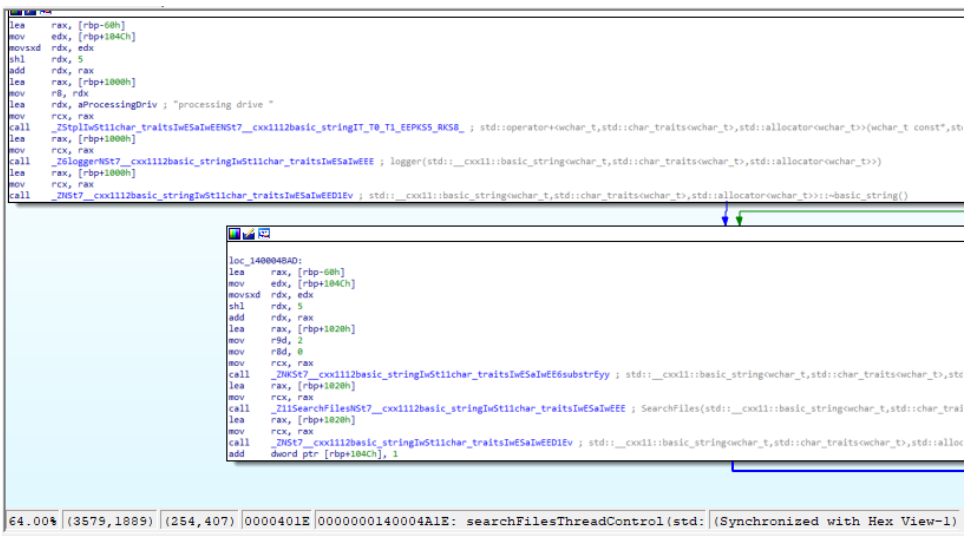
I files presi in considerazione vengono salvati in una variabile di *filesArray*, nel caso in cui vi siano errori di accesso agli stessi, viene prodotta una stringa di errore:



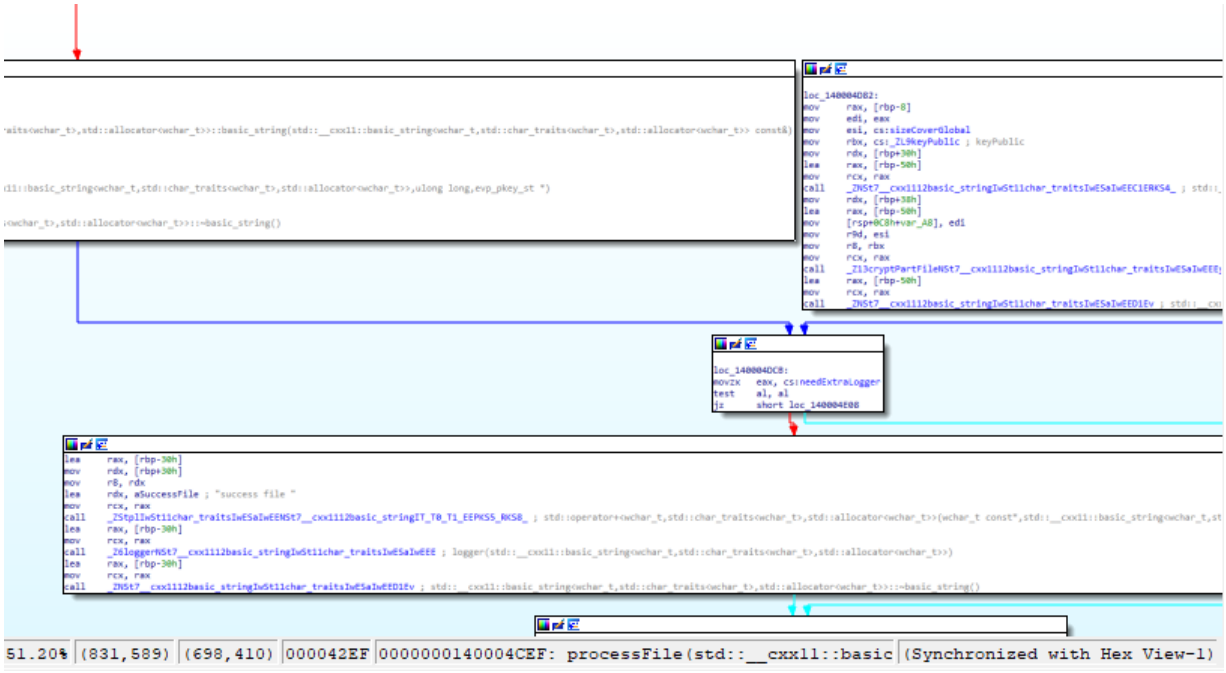




Qui un dettaglio di logging di infezione di un disco:

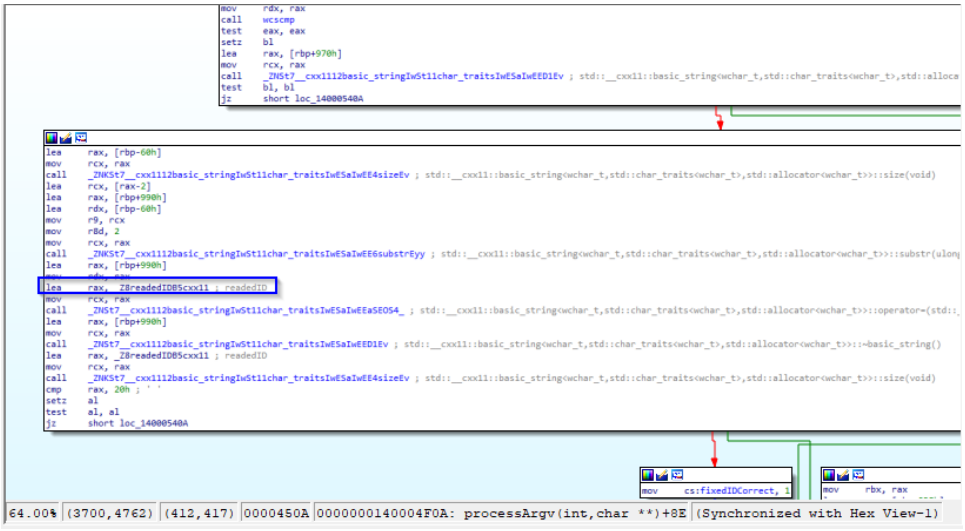


Qui un riferimento all'oggetto contenente la chiave pubblica:



L'operazione di lettura del file C:\ProgramData*ntuser.dat* risulta fondamentale per la decriptazione del ransomware stesso:

Qui, difatti, il riferimento all'ID di encryption del sample:

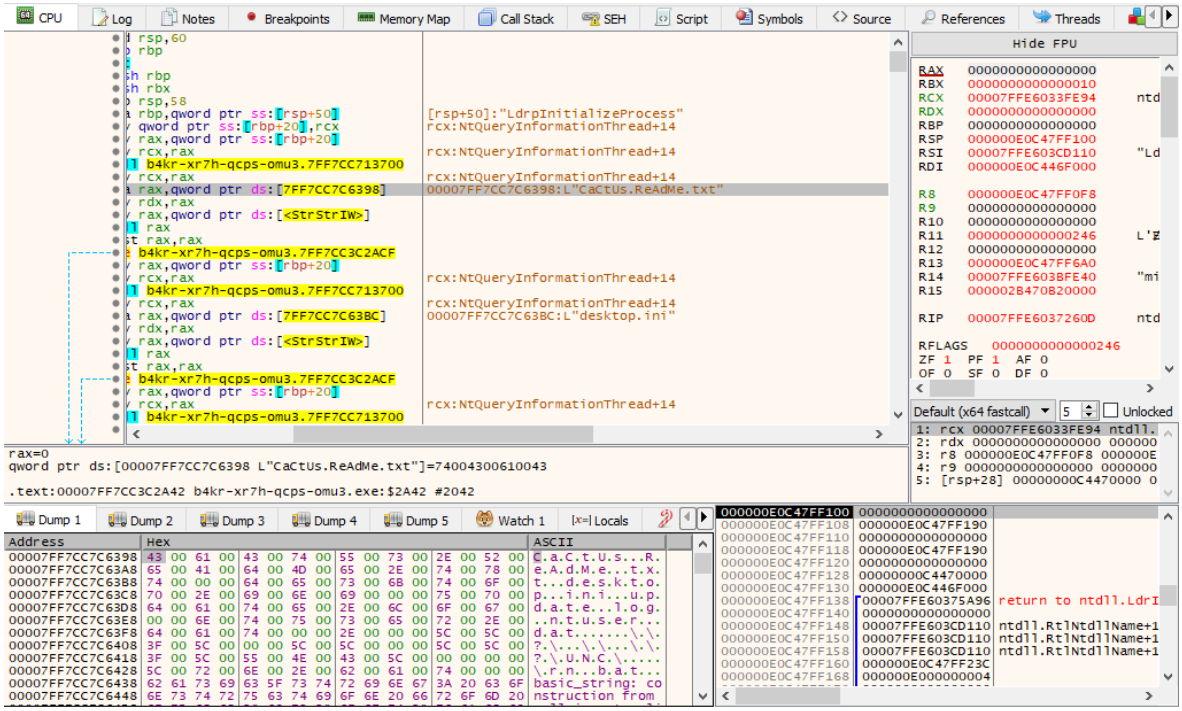


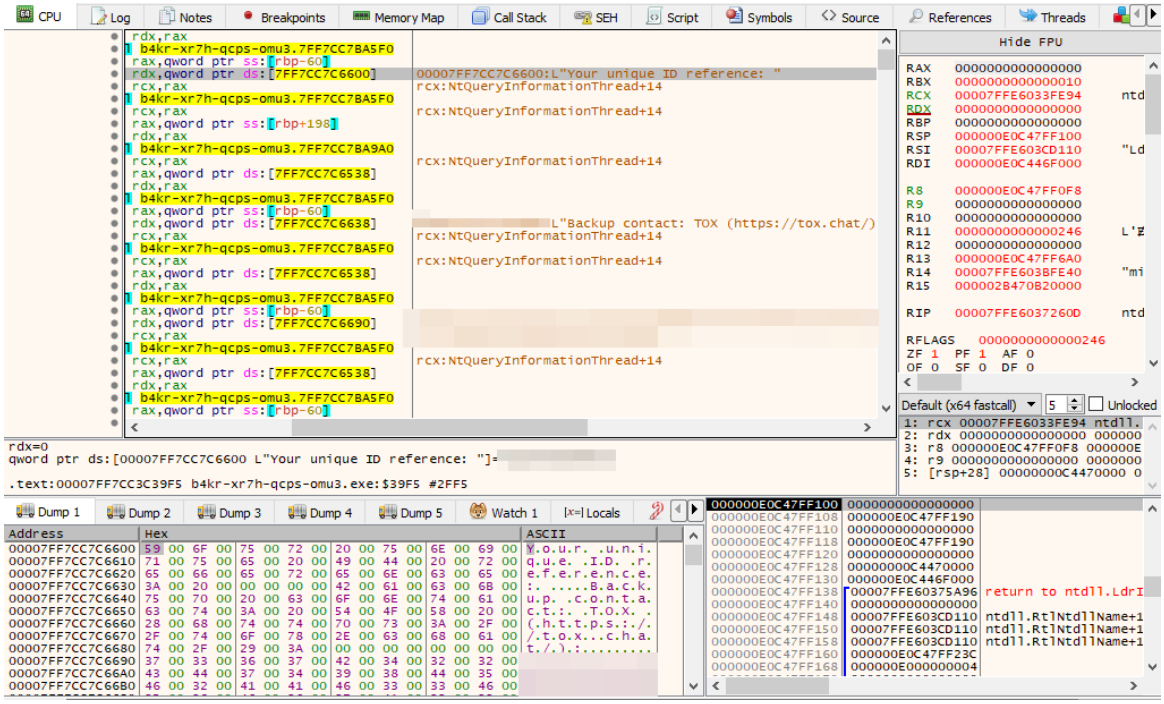
Qui i dettagli del codice esadecimale del sample analizzato, ove si evincono riferimenti a chars e strings management:

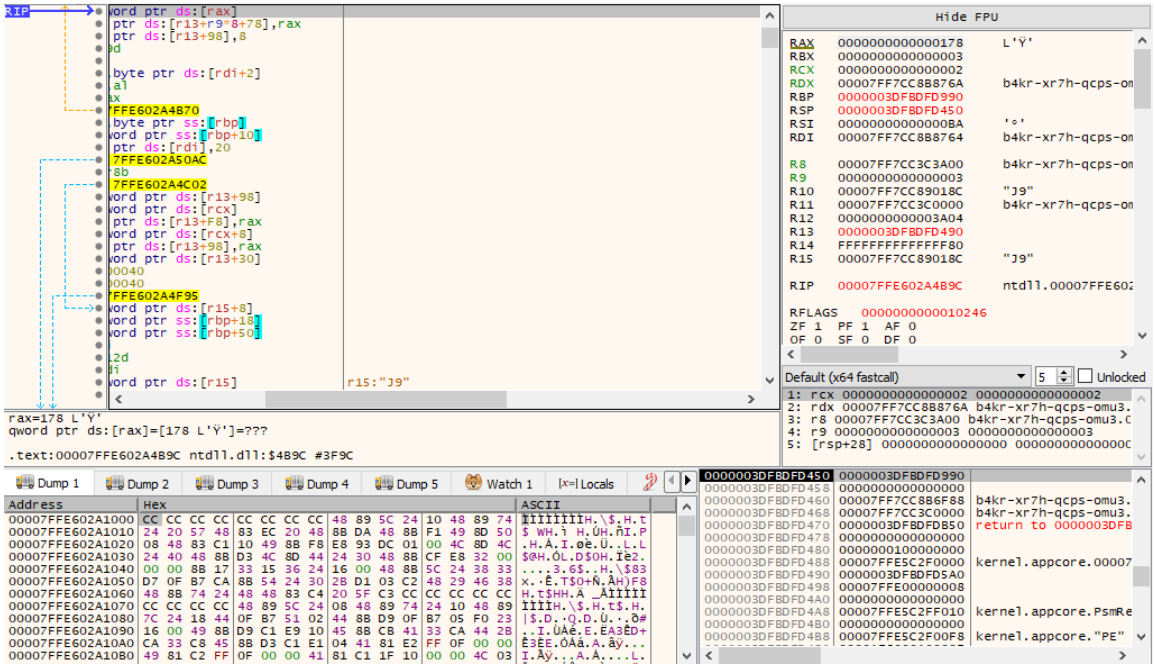
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00598DA0	23	00	00	00	4C	5F	4D	5F	63	6F	6E	73	74	72	75	63	#...L_M_construc
00598DB0	74	3C	63	68	61	72	20	63	6F	6E	73	74	2A	3E	00	0D	t<char const*>..
00598DC0	D9	07	5F	5A	4E	53	74	37	5F	5F	63	78	78	31	31	31	Ù_ZNSt7__cxx111
00598DD0	32	62	61	73	69	63	5F	73	74	72	69	6E	67	49	63	53	2basic_stringIcS
00598DE0	74	31	31	63	68	61	72	5F	74	72	61	69	74	73	49	63	t11char_traitsIc
00598DF0	45	53	61	49	63	45	45	31	32	5F	4D	5F	63	6F	6E	73	ESaIcEE12_M_cons
00598E00	74	72	75	63	74	49	50	4B	63	45	45	76	54	5F	53	38	tructIPKcEEvT_S8
00598E10	5F	53	74	32	30	66	6F	72	77	61	72	64	5F	69	74	65	_St20forward_ite
00598E20	72	61	74	6F	72	5F	74	61	67	00	C3	9D	00	00	D8	9D	rator_tag.Ã ..Ø
00598E30	00	00	05	E1	1C	00	00	2F	F0	01	00	02	C5	36	02	00	..á ../ð. Å6 .
00598E40	01	2F	F0	01	00	01	2F	F0	01	00	01	47	23	00	00	00	/ð /ð G#...
00598E50	13	A8	20	00	00	05	7A	02	07	5F	5A	4E	53	74	37	5F	¨ z _ZNSt7_
00598E60	5F	63	78	78	31	31	31	32	62	61	73	69	63	5F	73	74	_cxx1112basic_st
00598E70	72	69	6E	67	49	63	53	74	31	31	63	68	61	72	5F	74	ringIcSt11char_t
00598E80	72	61	69	74	73	49	63	45	53	61	49	63	45	45	43	34	raitsIcESaIcEEC4
00598E90	49	53	33	5F	45	45	50	4B	63	52	4B	53	33	5F	00	01	IS3_EEPKcRKS3_.
00598EA0	30	9E	00	00	40	9E	00	00	02	C5	36	02	00	01	2F	F0	0..@.. Å6 ./ð
00598EB0	01	00	01	5C	2D	02	00	00	13	A8	20	00	00	05	91	02	..\- ..¨ ...'
00598EC0	07	5F	5A	4E	53	74	37	5F	5F	63	78	78	31	31	31	32	_ZNSt7__cxx1112
00598ED0	62	61	73	69	63	5F	73	74	72	69	6E	67	49	63	53	74	basic_stringIcSt
00598EE0	31	31	63	68	61	72	5F	74	72	61	69	74	73	49	63	45	11char_traitsIcE
00598EF0	53	61	49	63	45	45	43	34	49	53	33	5F	45	45	79	63	SaIcEEC4IS3_EEyc
00598F00	52	4B	53	33	5F	00	01	97	9E	00	00	AC	9E	00	00	02	RKS3_.. ..¬..
00598F10	C5	36	02	00	01	37	56	00	00	01	93	00	00	00	01	5C	Å6 ..7V.. ...\
00598F20	2D	02	00	00	05	8D	21	00	00	93	00	00	00	58	11	24	- .. !... ...X $
00598F30	00	00	B4	10	00	00	58	49	23	00	00	E0	1E	00	00	00	..´. ..XI#..à ...
00598F40	07	55	54	00	00	41	62	61	73	69	63	5F	73	74	72	69	UT..Abasic_stri
00598F50	6E	67	3C	77	63	68	61	72	5F	74	2C	20	73	74	64	3A	ng<wchar_t, std:
00598F60	3A	63	68	61	72	5F	74	72	61	69	74	73	3C	77	63	68	:char_traits<wch
00598F70	61	72	5F	74	3E	2C	20	73	74	64	3A	3A	61	6C	6C	6F	ar_t>, std::allo
00598F80	63	61	74	6F	72	3C	77	63	68	61	72	5F	74	3E	20	3E	cator<wchar_t> >
00598F90	00	20	05	55	0B	3A	EE	00	00	4E	F9	20	00	00	08	05	. U :î..Nù ..
00598FA0	C0	0E	7A	A0	00	00	43	67	22	00	00	25	F9	20	00	00	À z ..Cg"..%ù ...
00598FB0	05	C7	02	5F	5A	4E	53	74	37	5F	5F	63	78	78	31	31	Ç _ZNSt7__cxx11
00598FC0	31	32	62	61	73	69	63	5F	73	74	72	69	6E	67	49	77	12basic_stringIw
00598FD0	53	74	31	31	63	68	61	72	5F	74	72	61	69	74	73	49	St11char_traitsI
00598FE0	77	45	53	61	49	77	45	45	31	32	5F	41	6C	6C	6F	63	wESaIwEE12_Alloc
00598FF0	5F	68	69	64	65	72	43	34	45	50	77	52	4B	53	33	5F	_hiderC4EPwRKS3_
00599000	00	91	9F	00	00	A1	9F	00	00	02	1A	37	02	00	01	7A	.´..¡.. ..7 ..z
00599010	A0	00	00	01	8E	2D	02	00	00	25	F9	20	00	00	05	CB	..Ž- ..%ù ...Ë
00599020	02	5F	5A	4E	53	74	37	5F	5F	63	78	78	31	31	31	32	_ZNSt7__cxx1112
00599030	62	61	73	69	63	5F	73	74	72	69	6E	67	49	77	53	74	basic_stringIwSt
00599040	31	31	63	68	61	72	5F	74	72	61	69	74	73	49	77	45	11char_traitsIwE

Sessione di debugging

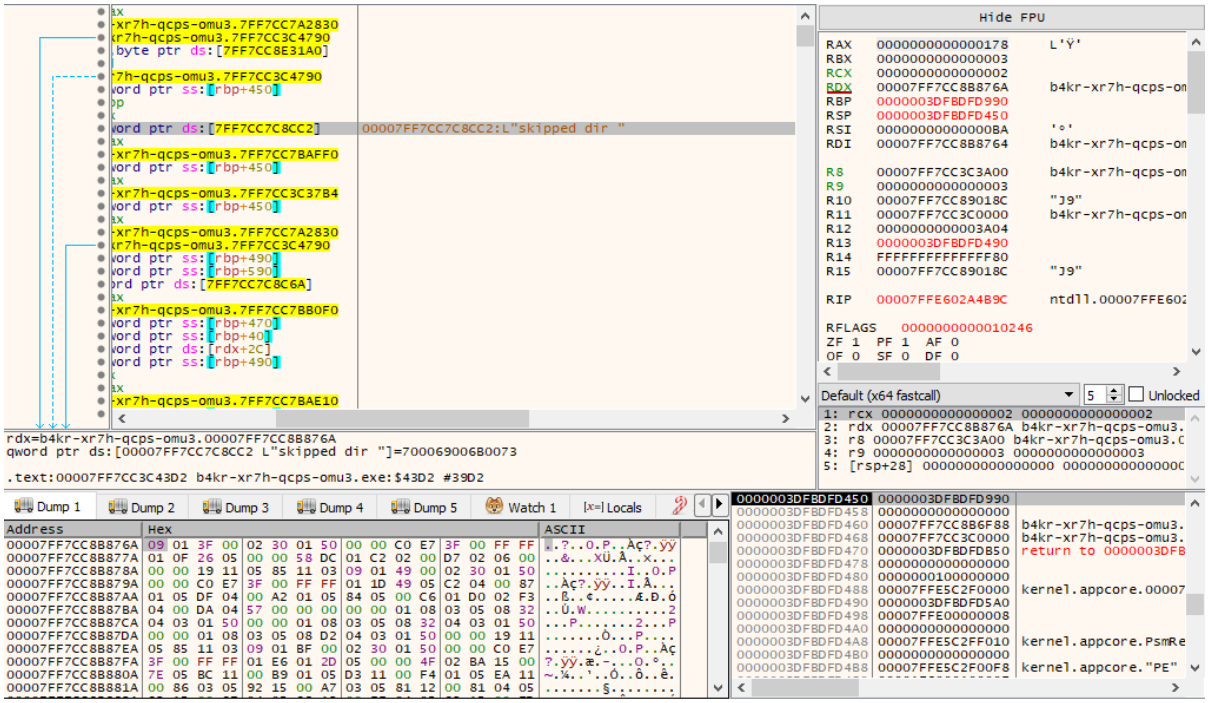
A seguire alcuni dettagli della sessione di debugging effettuata, ove si notano riferimenti al file TXT di readme di Cactus Ransomware, l'ID univoco dell'infezione ransomware, un riferimento a **TOX chat** per il contatto con i malcoders:



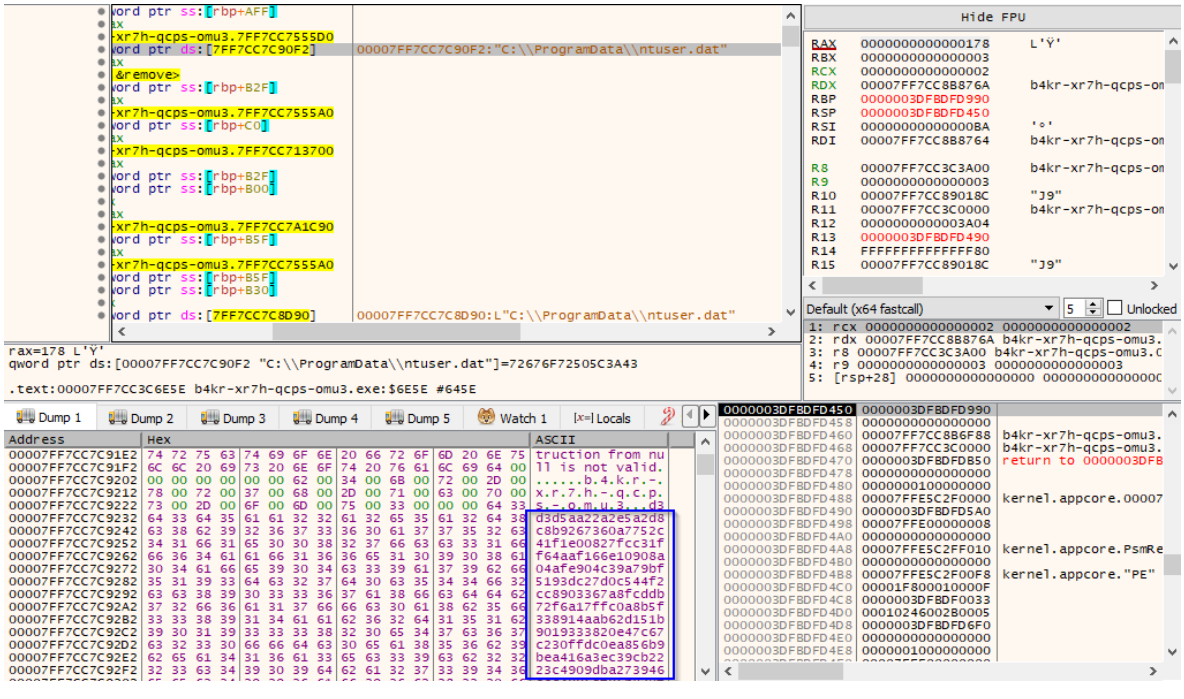


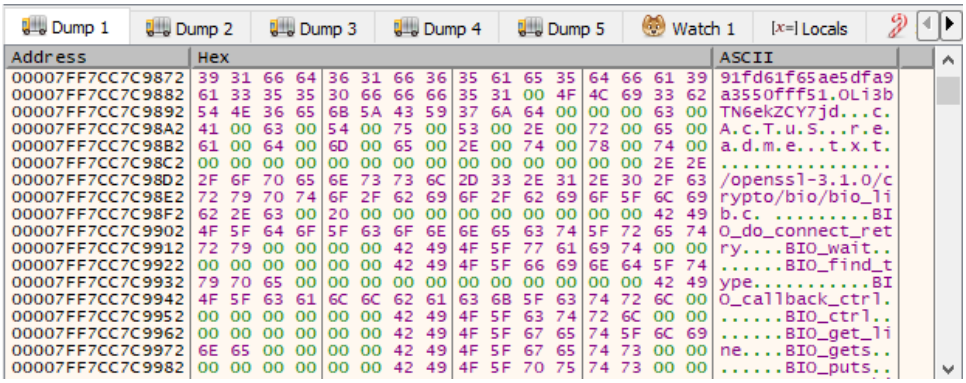


Nel caso in cui vengano presi in considerazione files e folders da non cifrare essi vengono "saltati" dal processo di encryption.

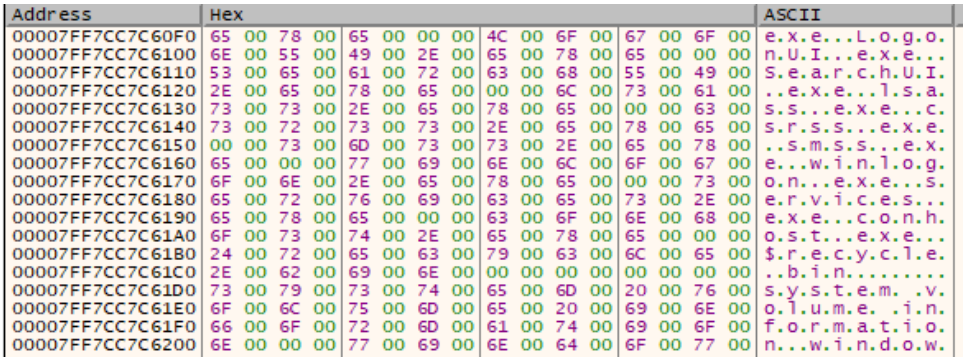


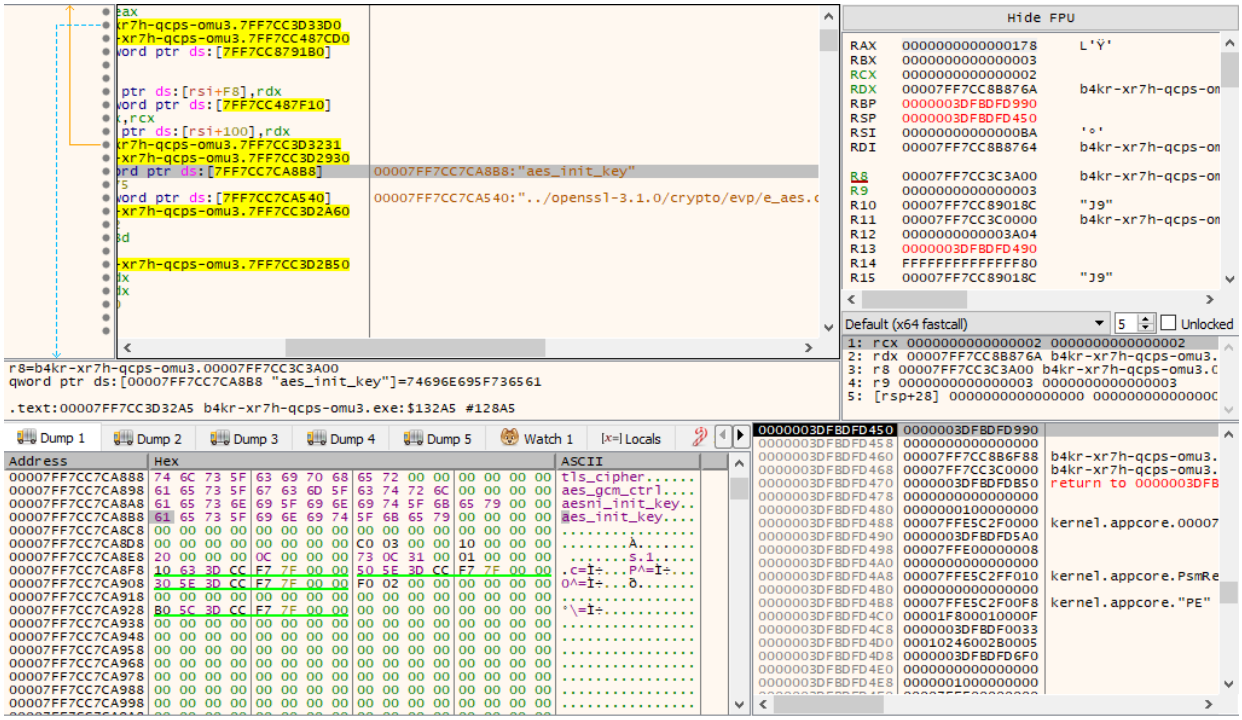
Il file C:\ProgramData\ntuser.dat contiene una stringa randomica che fa riferimento alla stringa di encryption del ransomware sample:



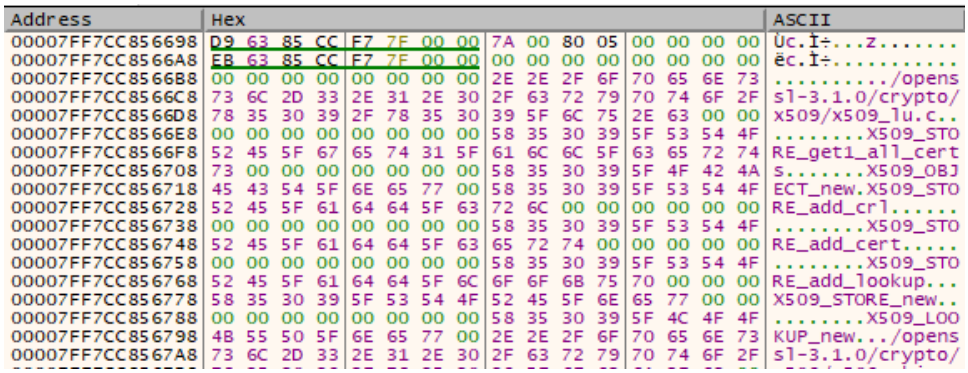


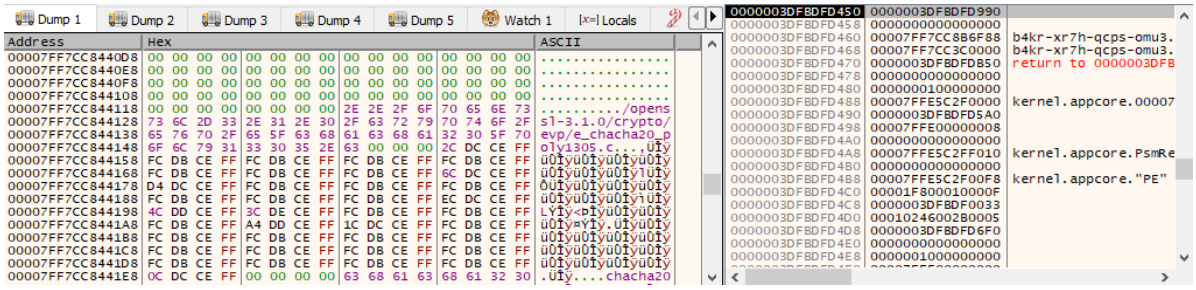
Qui i dettagli ASCII ed esadecimali dei processi presi in considerazione dall'infection kill chain e il richiamo della funzione di *AES_init_key*:

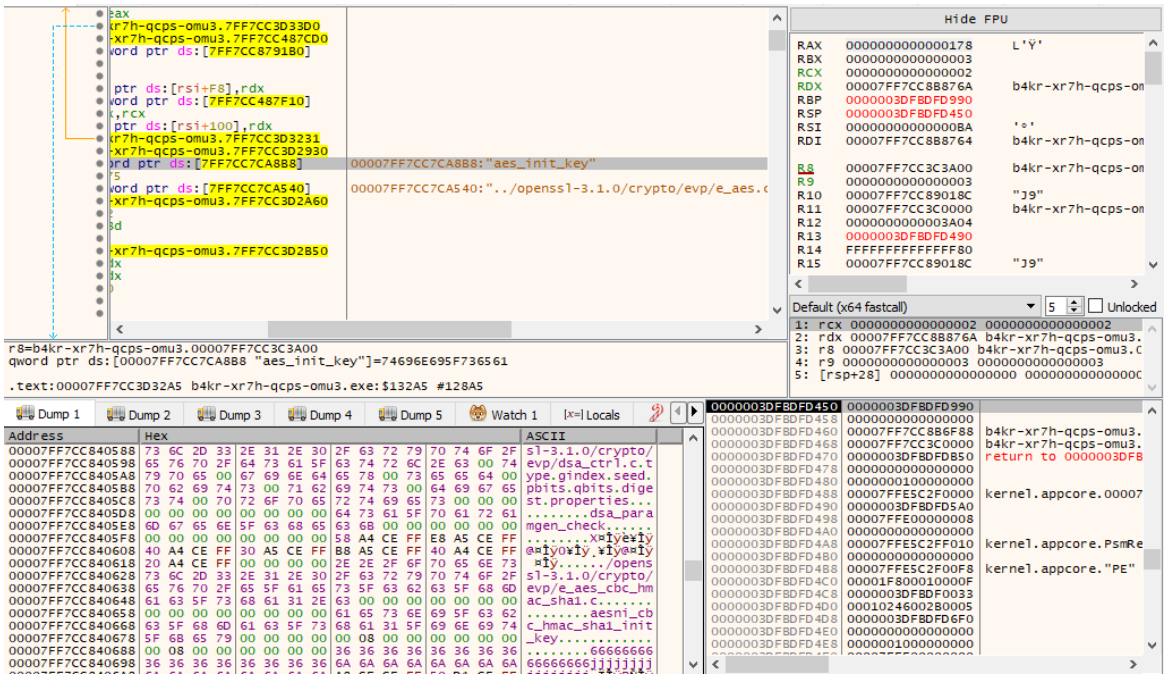




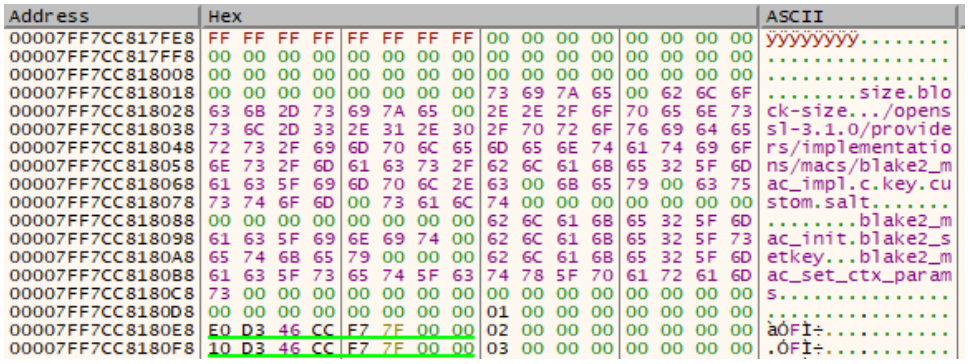
Qui possiamo notare encryption attributes di *OpenSSL* e *ChaCha20Poly1305*:



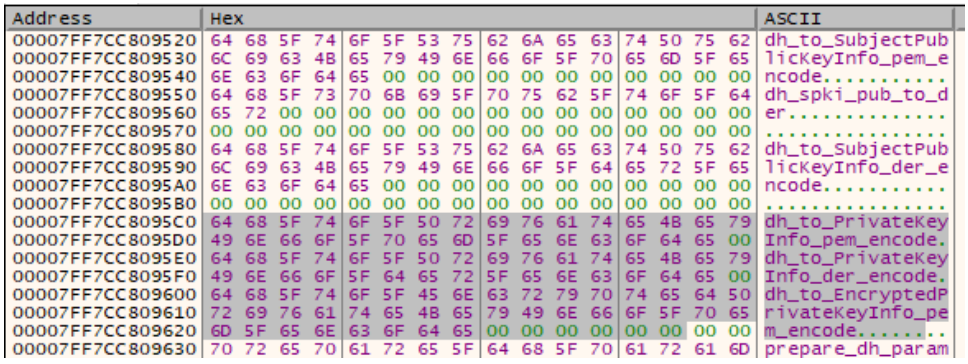




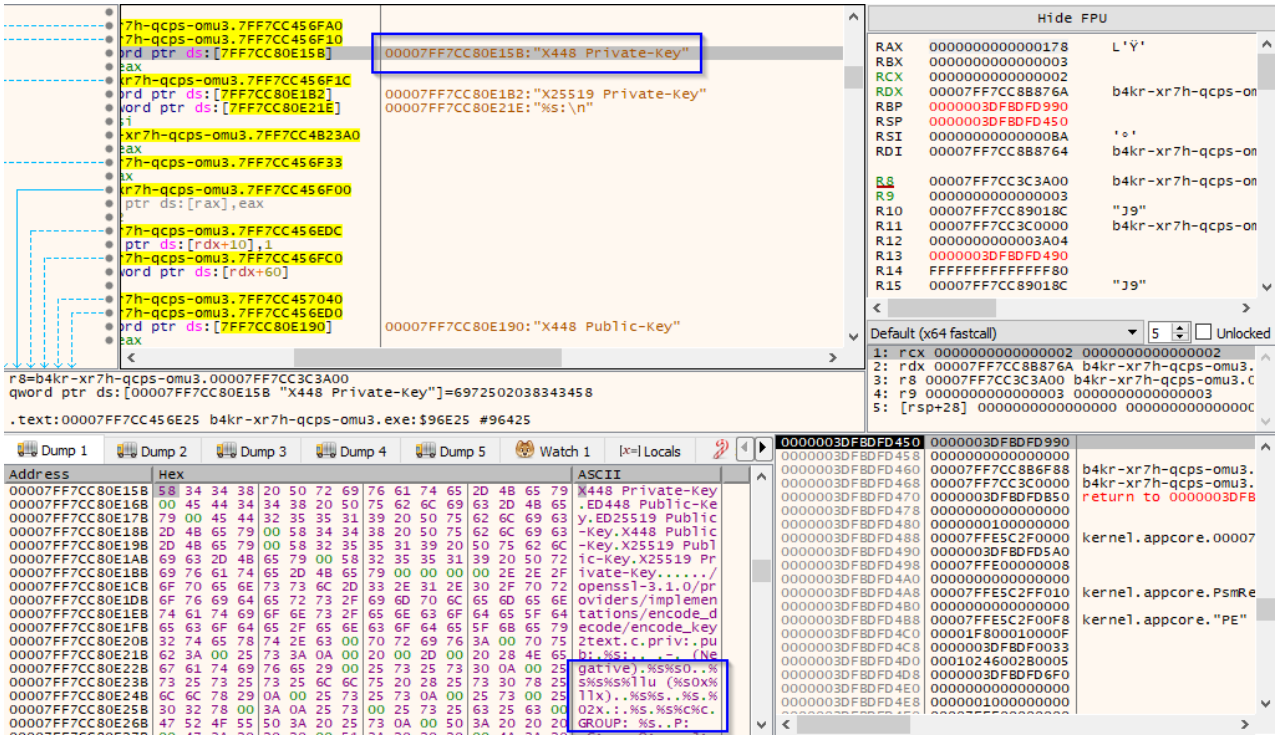
Si notino i dettagli in merito all'encryption routine Blake2 e l'inserimento della chiave privata con i tipi di dati ***%s (string)*** e ***%C (caratteri).***



Address	Hex	ASCII
00007FF7CC817FE8	FF FF FF FF FF FF FF FF 00 00 00 00 00 00 00 00	ÿÿÿÿÿÿÿÿ........
00007FF7CC817FF8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
00007FF7CC818008	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
00007FF7CC818018	00 00 00 00 00 00 00 00 73 69 7A 65 00 62 6C 6F	........size.blo
00007FF7CC818028	63 6B 2D 73 69 7A 65 00 2E 2E 2F 6F 70 65 6E 73	ck-size.../opens
00007FF7CC818038	73 6C 2D 33 2E 31 2E 30 2F 70 72 6F 76 69 64 65	sl-3.1.0/provide
00007FF7CC818048	72 73 2F 69 6D 70 6C 65 6D 65 6E 74 61 74 69 6F	rs/implementatio
00007FF7CC818058	6E 73 2F 6D 61 63 73 2F 62 6C 61 6B 65 32 5F 6D	ns/macs/blake2_m
00007FF7CC818068	61 63 5F 69 6D 70 6C 2E 63 00 6B 65 79 00 63 75	ac_impl.c.key.cu
00007FF7CC818078	73 74 6F 6D 00 73 61 6C 74 00 00 00 00 00 00 00	stom.salt.......
00007FF7CC818088	00 00 00 00 00 00 00 00 62 6C 61 6B 65 32 5F 6D	........blake2_m
00007FF7CC818098	61 63 5F 69 6E 69 74 00 62 6C 61 6B 65 32 5F 73	ac_init.blake2_s
00007FF7CC8180A8	65 74 6B 65 79 00 00 00 62 6C 61 6B 65 32 5F 6D	etkey...blake2_m
00007FF7CC8180B8	61 63 5F 73 65 74 5F 63 74 78 5F 70 61 72 61 6D	ac_set_ctx_param
00007FF7CC8180C8	73 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	s...............
00007FF7CC8180D8	00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00	....
00007FF7CC8180E8	E0 D3 46 CC F7 7F 00 00 02 00 00 00 00 00 00 00	àÓFÌ÷...........
00007FF7CC8180F8	10 D3 46 CC F7 7F 00 00 03 00 00 00 00 00 00 00	.ÓFÌ÷...........



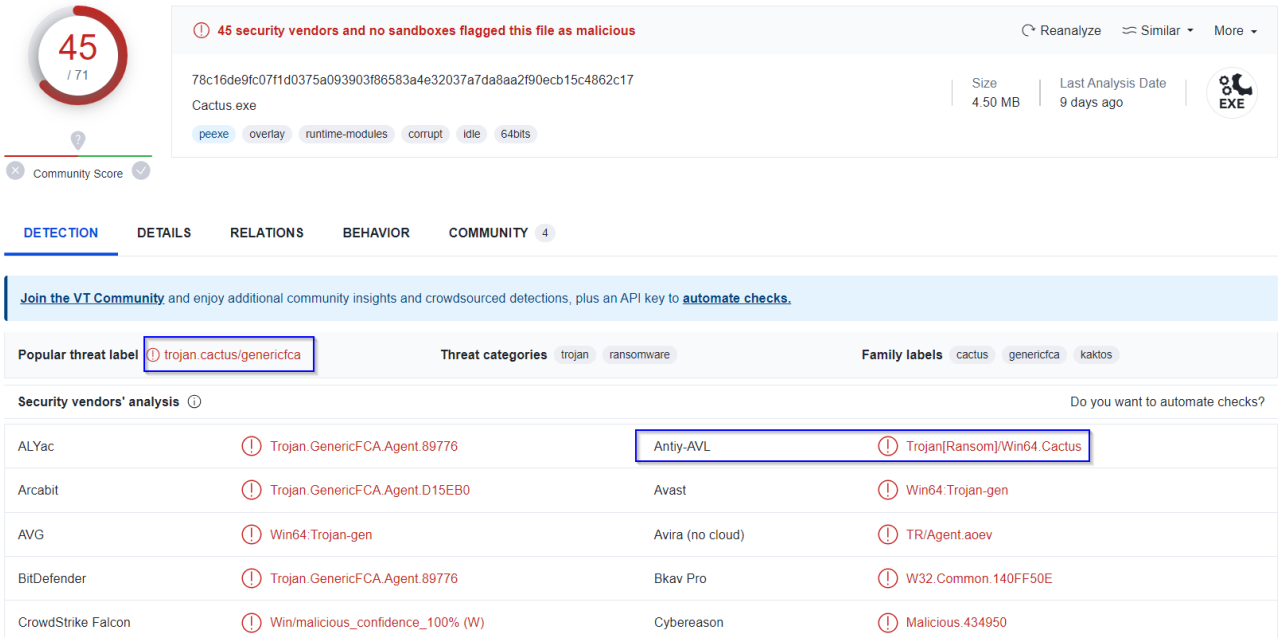
Address	Hex	ASCII
00007FF7CC809520	64 68 5F 74 6F 5F 53 75 62 6A 65 63 74 50 75 62	dh_to_SubjectPub
00007FF7CC809530	6C 69 63 4B 65 79 49 6E 66 6F 5F 70 65 6D 5F 65	licKeyInfo_pem_e
00007FF7CC809540	6E 63 6F 64 65 00 00 00 00 00 00 00 00 00 00 00	ncode...........
00007FF7CC809550	64 68 5F 73 70 6B 69 5F 70 75 62 5F 74 6F 5F 64	dh_spki_pub_to_d
00007FF7CC809560	65 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00	er..............
00007FF7CC809570	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
00007FF7CC809580	64 68 5F 74 6F 5F 53 75 62 6A 65 63 74 50 75 62	dh_to_SubjectPub
00007FF7CC809590	6C 69 63 4B 65 79 49 6E 66 6F 5F 64 65 72 5F 65	licKeyInfo_der_e
00007FF7CC8095A0	6E 63 6F 64 65 00 00 00 00 00 00 00 00 00 00 00	ncode...........
00007FF7CC8095B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
00007FF7CC8095C0	64 68 5F 74 6F 5F 50 72 69 76 61 74 65 4B 65 79	dh_to_PrivateKey
00007FF7CC8095D0	49 6E 66 6F 5F 70 65 6D 5F 65 6E 63 6F 64 65 00	Info_pem_encode.
00007FF7CC8095E0	64 68 5F 74 6F 5F 50 72 69 76 61 74 65 4B 65 79	dh_to_PrivateKey
00007FF7CC8095F0	49 6E 66 6F 5F 64 65 72 5F 65 6E 63 6F 64 65 00	Info_der_encode.
00007FF7CC809600	64 68 5F 74 6F 5F 45 6E 63 72 79 70 74 65 64 50	dh_to_EncryptedP
00007FF7CC809610	72 69 76 61 74 65 4B 65 79 49 6E 66 6F 5F 70 65	rivateKeyInfo_pe
00007FF7CC809620	6D 5F 65 6E 63 6F 64 65 00 00 00 00 00 00 00 00	m_encode........
00007FF7CC809630	70 72 65 70 61 72 65 5F 64 68 5F 70 61 72 61 6D	prepare_dh_param



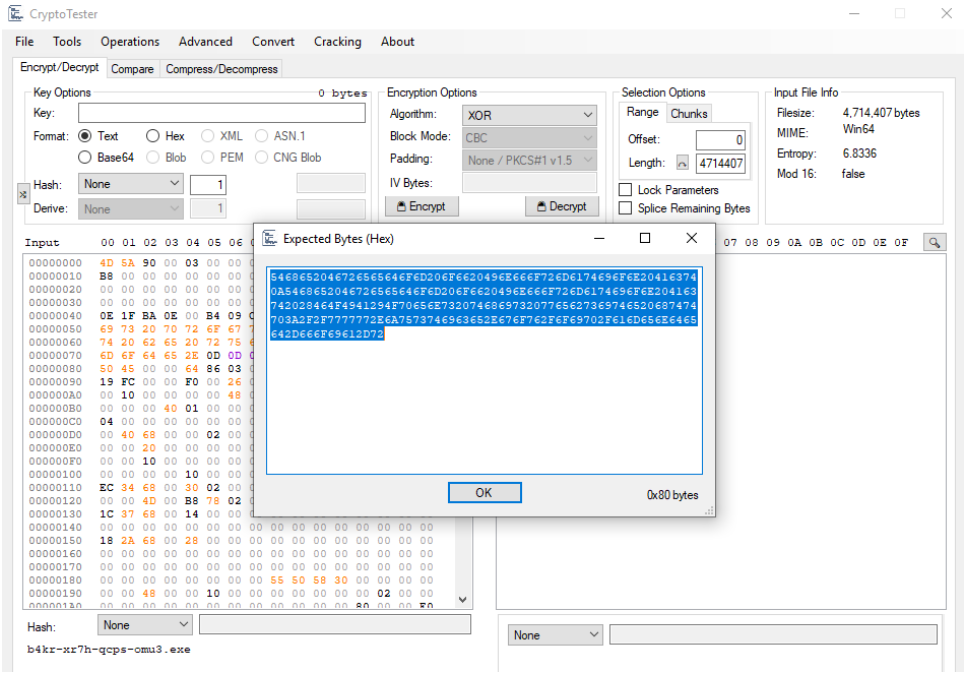
www.swascan.com | info@swascan.com

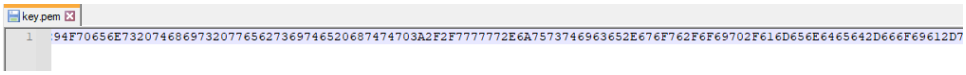
Threat research

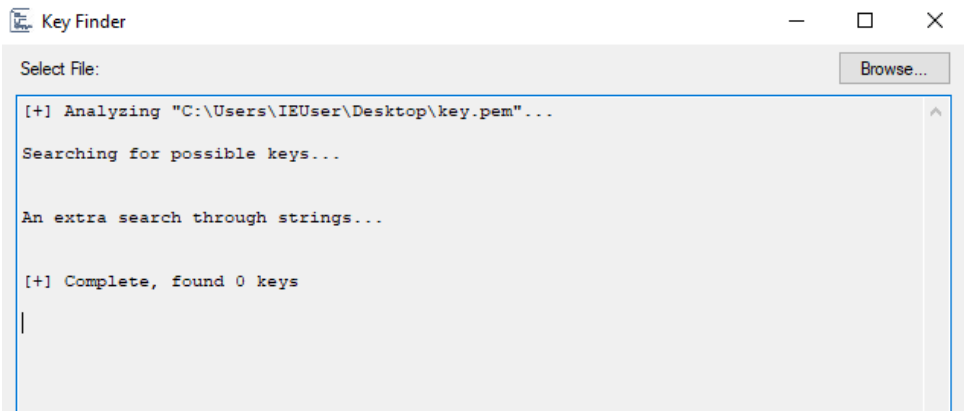
Il sample è riconosciuto come malevolo dalle fonti OSINT ed identificato come **trojan.cactus/genericfca:**



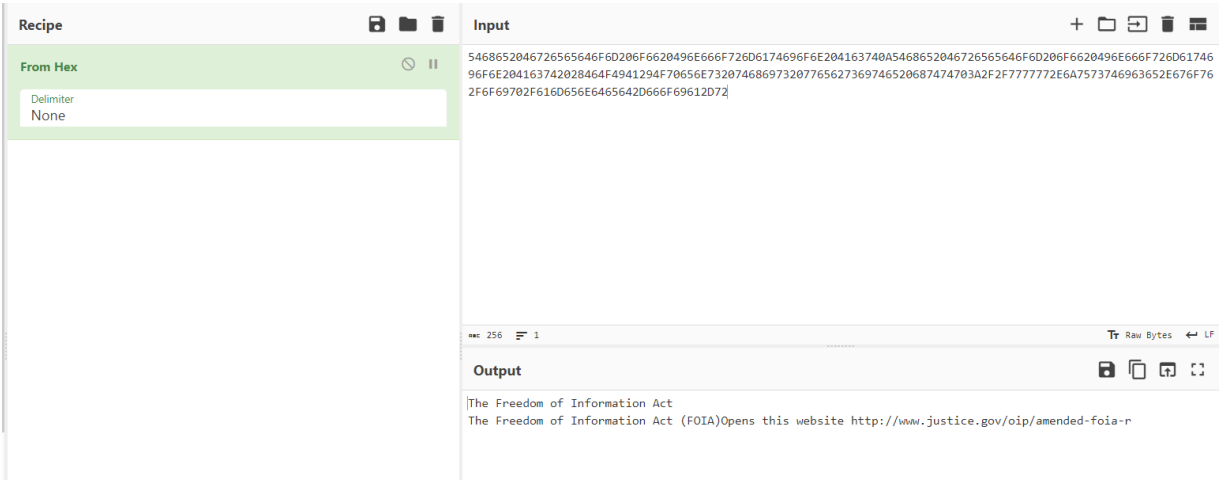
Qui un dettaglio di un key finding attempt mediante la stringa randomica inserita nel file **C:\ProgramData\ntuser.dat:**







Effettuando una decodifica dall'esadecimale della stringa in questione è possibile identificare il dominio di Freedom of Information Act ed il dominio justice[.]gov. Tuttavia, con i pattern successivi essa dovrebbe contenere la sottostringa utilizzata come chiave pubblica per la cifratura del ransomware.



Cactus Ransomware utilizza tecniche di Anti-VM basate sul CPUID:

Environment Awareness

The input sample contains a known anti-VM trick

details	Found VM detection artifact "CPUID trick" in "sample.bin" (Offset: 105697)
source	Binary File
relevance	5/10
ATT&CK ID	T1497 (Show technique in the MITRE ATT&CK™ matrix)

A seguire un dettaglio di caricamento dinamico del modulo di encryption bcryptprimitives.dll in un contesto di esecuzione:

Loads the cryptographic module DLL

details	"<Input Sample>.exe" loaded module "%WINDIR%\System32\bcryptprimitives.dll" at 41380000
source	Loaded Module
ATT&CK ID	T1027 (Show technique in the MITRE ATT&CK™ matrix)

Qui un dettaglio di enumerazione di librerie DLL utilizzate, nello specifico RSTRTMGR.DLL (per gestire eventuali files già in uso ad altri processi), NCRYPT.DLL e BCRYPT.DLL, WSOCK32.DLL (che gestisce connessioni sockets, con tutta probabilità adoperata anche in fase di connessioni

Command and Control), FLTLIB.DLL (utilizzabile per filtri e ricerche, anche in sede di files enumeration).

Tries to access non-existent files (executable)

details	"<Input Sample>.exe" trying to access non-existent file "C:\RSTRTMGR.DLL" "<Input Sample>.exe" trying to access non-existent file "C:\NCRYPT.DLL" "<Input Sample>.exe" trying to access non-existent file "C:\BCRYPT.DLL" "<Input Sample>.exe" trying to access non-existent file "C:\NTASN1.DLL" "<Input Sample>.exe" trying to access non-existent file "C:\WSOCK32.DLL" "<Input Sample>.exe" trying to access non-existent file "C:\FLTLIB.DLL" "<Input Sample>.exe" trying to access non-existent file "C:\CRYPTBASE.DLL"
source	API Call
relevance	3/10
ATT&CK ID	T1083 (Show technique in the MITRE ATT&CK™ matrix)

Qui le funzionalità di sockets connections:

Network Related

Contains ability to communicate with network (APIs)

details	Found api string "accept" (Indicator: "accept"; Source: "00000000-00004400-00000C1F-78593735") Found api string "connect" (Indicator: "connect"; Source: "00000000-00004400-00000C1F-78594094") Found api string "listen" (Indicator: "listen"; Source: "00000000-00004400-00000C1F-78594795") Found api string "socket" (Indicator: "socket"; Source: "00000000-00004400-00000C1F-78595669")
source	File/Memory
relevance	1/10
ATT&CK ID	T1071 (Show technique in the MITRE ATT&CK™ matrix)

Qui un'evidenza della lettura delle informazioni relative al language pack installato sulla macchina con il fine di identificare la potenziale nazionalità delle vittime:

Unusual Characteristics

Reads the windows installation language

details	"<Input Sample>.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\NLS\LANGUAGE GROUPS"; Key: "1")
source	Registry Access
relevance	2/10
ATT&CK ID	T1614.001 (Show technique in the MITRE ATT&CK™ matrix)

A seguire i dettagli di un Pulse (il quale rappresenta un IOC container) riferibile a diversi indicatori associati a Cactus Ransomware:

Cactus Ransomware IOCs | PasteNet - Powerful Notetaking

CREATED 2 MONTHS AGO by Bheeshmar | Public | TLP: Green

Cactus Ransomware is a Ransomware which is active since March 2023. They have launched their DLS on DarkWeb in July 2023.

REFERENCES: http://pastenet.com/oDU2sokV/
https://twitter.com/RakeshKrish12/status/1682236940073185282

TAGS: pastenet, pastebin, paste, manufacturing, iocs, cactus, ransomware, sonar, malware, databreach, dataleak

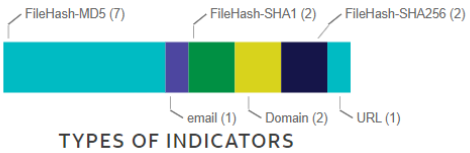
INDUSTRIES: Transportation, Food, Manufacturing, Construction, Marketing, Hardware, Nature

TARGETED COUNTRIES: United States of America, Italy, United Kingdom of Great Britain and Northern Ireland, Portugal, France, India, Switzerland

MALWARE FAMILIES: CACTUS, Cactus

ENDPOINT SECURITY Scan your endpoints for IOCs from this Pulse!

Indicators of Compromise (15) | Related Pulses (1) | Comments (0) | History (0)



TYPES OF INDICATORS

E' possibile avere contezza di un ulteriore dominio TOR, nello specifico sonarmsng5vzwqezlvtu2iiwwdn3dxkhotftikhowpfjuzg7p3ca5eid[.]onion e l'indirizzo e-mail di contatto cactus787835[@]proton[.]me:

TYPE	INDICATOR	ROLE	TITLE	ADDED	ACTIVE	RELATED PULSES
email	cactus787835@proton.me			Jul 21, 2023, 4:00:45 AM		0
domain	sonarmsng5vzwqezlvtu2iiwwdn3dxkhotftikhowpfjuzg7p3ca5eid.onion			Jul 21, 2023, 4:00:45 AM		1
domain	cactusbloguuodvqjmnzlwetjlpj6aggc6iocwhuupb47laukux7ckid.onion			Jul 21, 2023, 4:00:45 AM		0
URL	http://sonarmsng5vzwqezlvtu2iiwwdn3dxkhotftikhowpfjuzg7p3ca5eid.onion/cont...			Jul 21, 2023, 4:00:45 AM		0
FileHash-SHA256	c52ad663ff29e146de6b7b20d834304202de7120e93a93de1de1cb1d56190bfd		RC6_Constants	Jul 21, 2023, 4:00:45 AM		0
FileHash-SHA256	78c16de9fc07f1d0375a093903f86583a4e32037a7da8aa2f90ecb15c4862c17		RC6_Constants	Jul 21, 2023, 4:00:45 AM		0
FileHash-SHA1	cb570234349507a204c558fc8c4ecf713e2c0ac3		RC6_Constants	Jul 21, 2023, 4:00:45 AM		0
FileHash-SHA1	173f9b0db97097676a028b4b877630adc7281d2f		RC6_Constants	Jul 21, 2023, 4:00:45 AM		0
FileHash-MD5	eba1596272ff695a1219b1380468293a			Jul 21, 2023, 4:00:45 AM		0
FileHash-MD5	e28db6a65da2ebcf304873c9a5ed086d		RC6_Constants	Jul 21, 2023, 4:00:45 AM		0

TYPE	INDICATOR	ROLE	TITLE	ADDED	ACTIVE	RELATED PULSES
FileHash-MD5	de6ce47e28337d28b6d29ff61980b2e9		RC6_Constants	Jul 21, 2023, 4:00:45 AM		0
FileHash-MD5	949d9523269604db26065f002feef9ae			Jul 21, 2023, 4:00:45 AM		0
FileHash-MD5	5737cb3a9a6d22e957cf747986eeb1b3			Jul 21, 2023, 4:00:45 AM		0
FileHash-MD5	2611833c12aa97d3b14d2ed541df06b2			Jul 21, 2023, 4:00:45 AM		0
FileHash-MD5	1add9766eb649496bc2fa516902a5965			Jul 21, 2023, 4:00:45 AM		0

IOCs

- 78c16de9fc07f1d0375a093903f86583a4e32037a7da8aa2f90ecb15c4862c17
- cb570234349507a204c558fc8c4ecf713e2c0ac3
- e28db6a65da2ebcf304873c9a5ed086d
- Updates Check Task scheduled task
- CaCtUs.ReAdMe.txt
- cactus[@]mexicomail[.]com
- TOX Chat ID: 7367B422CD7498D5F2AAF33F58F67A332F8520CF0279A5FBB4611E0121AE421AE1D49ACEABB254686
- cactus787835[@]proton[.]me
- cactusbloguuodvqjmnzlwetjlpj6aggc6iocwhuupb47laukux7ckid[.]onion
- sonarmsng5vzwqezlvtu2iiwwdn3dxkhotftikhowpfjuzg7p3ca5eid[.]onion

Regola YARA

```
rule CactusRule

{

    strings:

        $cactusStr = "CaCtUs.ReAdMe.txt"

        $cactusHex = { 43 61 43 74 55 73 2e 52 65 41 64 4d 65 2e 74 78 74 }


    condition:

        $cactusStr or $cactusHex

}
```

Conclusioni

Cactus Ransomware possiede numerose caratteristiche che, almeno potenzialmente, potrebbero cambiare lo scenario delle nuove infezioni ransomware. I nuovi threats assumerebbero nuove caratteristiche fondamentali di auto-encryption ed il cambio consecutivo di più estensioni dei files criptati, questo per rendere più difficoltosa l'identificazione dei files stessi, sottoposti al processo di cifratura. È inoltre presente una peculiarità relativa all'utilizzo del file C:\ProgramData\ntuser.dat al fine di archiviare la stringa utilizzata come chiave pubblica per la crittografia del malware sample stesso. Il file ntuser.dat rappresenta un elemento utilizzato ad-hoc per la self-encryption del ransomware appositamente con tale filename con lo scopo probabilmente di confondere ed effettuare evasion. Per comprendere la natura ed il funzionamento di Cactus Ransomware possiamo citare due particolarità importanti: esso utilizza il packer UPX, il quale è largamente conosciuto e semplice da "unpackare". Inoltre, i files sottoposti al processo di encryption, vengono divisi in porzioni salvate in microbuffers, probabilmente per velocizzare la gestione dei data streams criptati. Dalle evidenze dei real-world scenarios si evince una volontà da parte di Cactus Ransomware di effettuare due principali tasks di discovery incrociati con lo scopo di riuscire più facilmente ad ottenere informazioni e dettagli in merito alle utenze ed al dominio anche nel caso in cui ci sia la detection (ed eventualmente il blocco preventivo) di una delle metodologie utilizzate, come ad esempio il tool di scansione SoftPerfect Network Scanner.

Riferimenti

[0]: Cactus Ransomware Group Adds Four New Victims (privacyaffairs.com)

[1]: What is CACTUS Ransomware? (lepide.com)