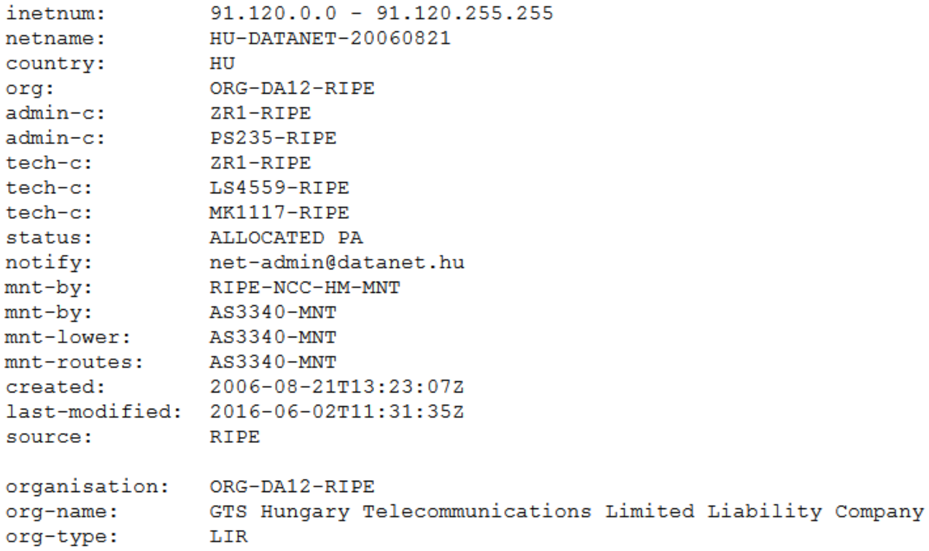
A look at Cerber Ransomware

Cerber is currently been delivered through RIG EK and appears fast and simple.

The sample I looked at was found been delivered through Rig EK (“waterhole”), a compromised site served it as a delivery method.

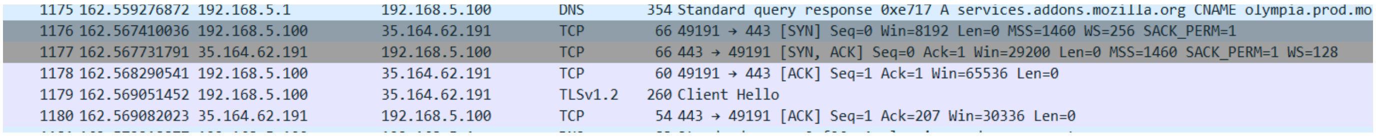
Looking at the packet capture I saw

- A list of more than 200 host ip addesses (91.119.56.0 - 91.121.59.255)
- a lot of UDP traffic going to Hungry
- ports 53, 137 , 138, 5355, 6892



```
inetnum:        91.120.0.0 - 91.120.255.255
netname:        HU-DATANET-20060821
country:        HU
org:            ORG-DA12-RIPE
admin-c:        ZR1-RIPE
admin-c:        PS235-RIPE
tech-c:         ZR1-RIPE
tech-c:         LS4559-RIPE
tech-c:         MK1117-RIPE
status:         ALLOCATED PA
notify:         net-admin@datanet.hu
mnt-by:         RIPE-NCC-HM-MNT
mnt-by:         AS3340-MNT
mnt-lower:      AS3340-MNT
mnt-routes:     AS3340-MNT
created:        2006-08-21T13:23:07Z
last-modified:  2016-06-02T11:31:35Z
source:         RIPE

organisation:   ORG-DA12-RIPE
org-name:       GTS Hungary Telecommunications Limited Liability Company
org-type:       LIR
```

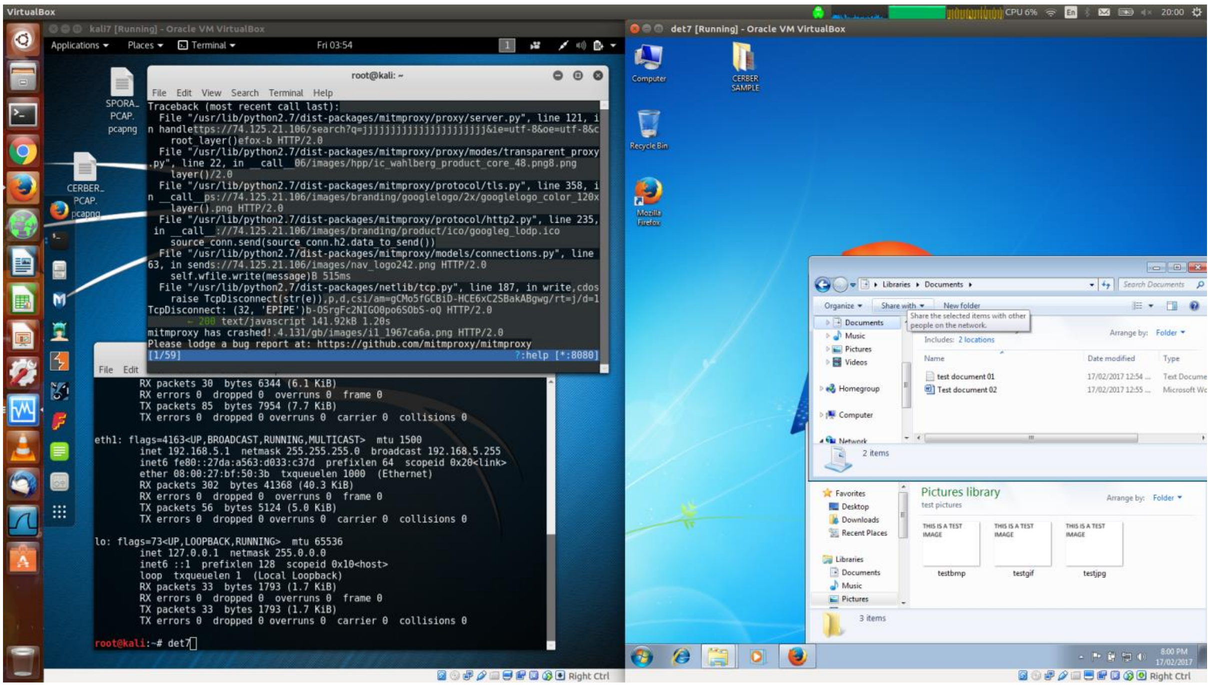
- I also observed TCP packets to Amazon services 35 network, 52 network



```
1175 162.559276872 192.168.5.1     192.168.5.100   DNS      354 Standard query response 0xe717 A services.addons.mozilla.org CNAME olympia.prod.mo
1176 162.567410036 192.168.5.100   35.164.62.191   TCP       66 49191 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1177 162.567731791 35.164.62.191   192.168.5.100   TCP       66 443 → 49191 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
1178 162.568290541 192.168.5.100   35.164.62.191   TCP       60 49191 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
1179 162.569051452 192.168.5.100   35.164.62.191   TLSv1.2  260 Client Hello
1180 162.569082023 35.164.62.191   192.168.5.100   TCP       54 443 → 49191 [ACK] Seq=1 Ack=207 Win=30336 Len=0
```

  - Cypher keys appeared to be exchanged along 54 (amazon network)

The Sample I had appeared to only effect word documents and may have been targeted to that to allow for faster encryption.

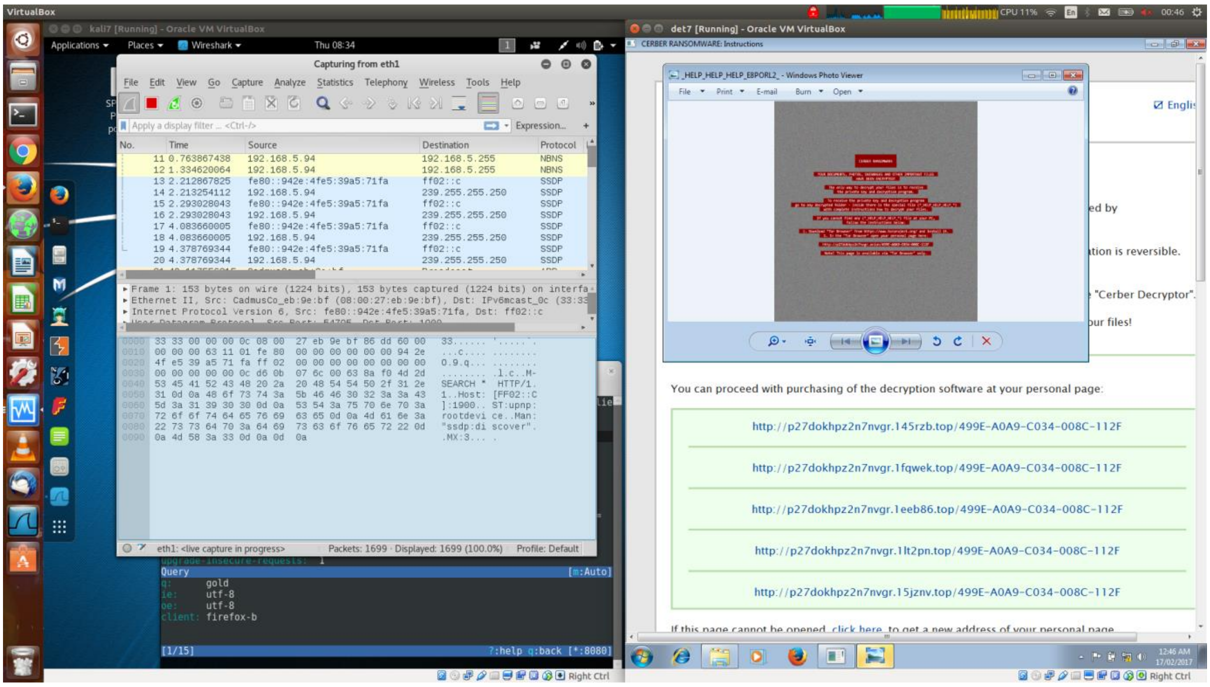


```
Traceback (most recent call last):
  File "/usr/lib/python2.7/dist-packages/mitmproxy/proxy/server.py", line 121, i
n handlettps://74.125.21.106/search?q=jjjjjjjjjjjjjjjjjjjjjj&ie=utf-8&oe=utf-8&c
    root_layer()efox-b HTTP/2.0
  File "/usr/lib/python2.7/dist-packages/mitmproxy/proxy/modes/transparent_proxy
.py", line 22, in __call__06/images/hpp/ic_wahlberg_product_core_48.png8.png
    layer()/2.0
  File "/usr/lib/python2.7/dist-packages/mitmproxy/protocol/tls.py", line 358, i
n __call__ps://74.125.21.106/images/branding/googlelogo/2x/googlelogo_color_120x
    layer().png HTTP/2.0
  File "/usr/lib/python2.7/dist-packages/mitmproxy/protocol/http2.py", line 235,
 in __call__://74.125.21.106/images/branding/product/ico/googleg_lodp.ico
    source_conn.send(source_conn.h2.data_to_send())
  File "/usr/lib/python2.7/dist-packages/mitmproxy/models/connections.py", line
63, in sends://74.125.21.106/images/nav_logo242.png HTTP/2.0
    self.wfile.write(message)B 515ms
  File "/usr/lib/python2.7/dist-packages/netlib/tcp.py", line 187, in write,cdos
    raise TcpDisconnect(str(e)),p,d,csi/am=gCMo5fGCBiD-HCE6xC2SBakABgwg/rt=j/d=1
TcpDisconnect: (32, 'EPIPE')b-OSrgFc2NIGO0po6SObS-oQ HTTP/2.0
       ← 200 text/javascript 141.92kB 1.20s
mitmproxy has crashed!.4.131/gb/images/i1_1967ca6a.png HTTP/2.0
Please lodge a bug report at: https://github.com/mitmproxy/mitmproxy
[1/59]                                                          ?:help [*:8080]
```

```
        RX packets 30  bytes 6344 (6.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 85  bytes 7954 (7.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.5.1  netmask 255.255.255.0  broadcast 192.168.5.255
        inet6 fe80::27da:a563:d033:c37d  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:bf:50:3b  txqueuelen 1000  (Ethernet)
        RX packets 302  bytes 41368 (40.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 56  bytes 5124 (5.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 33  bytes 1793 (1.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 33  bytes 1793 (1.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# det7
```

- Sample photo showing
  - (right side)test documents and pictures pre execution
  - (left side) kali proxy testing and network settings

Cerber appears very simple which makes it easily marketable, upon execution you are presented with the changed desktop image (right) and personal addresses which are accessible as tor addressing.



```
No.  Time          Source                       Destination       Protocol
  11 0.763867438   192.168.5.94                 192.168.5.255     NBNS
  12 1.334620064   192.168.5.94                 192.168.5.255     NBNS
  13 2.212867825   fe80::942e:4fe5:39a5:71fa    ff02::c           SSDP
  14 2.213254112   192.168.5.94                 239.255.255.250   SSDP
  15 2.293028043   fe80::942e:4fe5:39a5:71fa    ff02::c           SSDP
  16 2.293028043   192.168.5.94                 239.255.255.250   SSDP
  17 4.083660005   fe80::942e:4fe5:39a5:71fa    ff02::c           SSDP
  18 4.083660005   192.168.5.94                 239.255.255.250   SSDP
  19 4.378769344   fe80::942e:4fe5:39a5:71fa    ff02::c           SSDP
  20 4.378769344   192.168.5.94                 239.255.255.250   SSDP

▸ Frame 1: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interfa
▸ Ethernet II, Src: CadmusCo_eb:9e:bf (08:00:27:eb:9e:bf), Dst: IPv6mcast_0c (33:33
▸ Internet Protocol Version 6, Src: fe80::942e:4fe5:39a5:71fa, Dst: ff02::c

0000  33 33 00 00 00 0c 08 00  27 eb 9e bf 86 dd 60 00   33...... '.....`.
0010  00 00 00 63 11 01 fe 80  00 00 00 00 00 00 94 2e   ...c.... ........
0020  4f e5 39 a5 71 fa ff 02  00 00 00 00 00 00 00 00   O.9.q... ........
0030  00 00 00 00 00 0c d6 0b  07 6c 00 63 8a f0 4d 2d   ........ .l.c..M-
0040  53 45 41 52 43 48 20 2a  20 48 54 54 50 2f 31 2e   SEARCH *  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  5b 46 46 30 32 3a 3a 43   1..Host: [FF02::C
0060  5d 3a 31 39 30 30 0d 0a  53 54 3a 75 70 6e 70 3a   ]:1900.. ST:upnp:
0070  72 6f 6f 74 64 65 76 69  63 65 0d 0a 4d 61 6e 3a   rootdevi ce..Man:
0080  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover".
0090  0a 4d 58 3a 33 0d 0a 0d  0a                        .MX:3... .

eth1: <live capture in progress>   Packets: 1699 · Displayed: 1699 (100.0%)   Profile: Default
```

```
Query                                                        [m:Auto]
q:      gold
ie:     utf-8
oe:     utf-8
client: firefox-b

[1/15]                                     ?:help q:back [*:8080]
```

ed by

tion is reversible.

"Cerber Decryptor".

ur files!

You can proceed with purchasing of the decryption software at your personal page:

http://p27dokhpz2n7nvgr.145rzb.top/499E-A0A9-C034-008C-112F

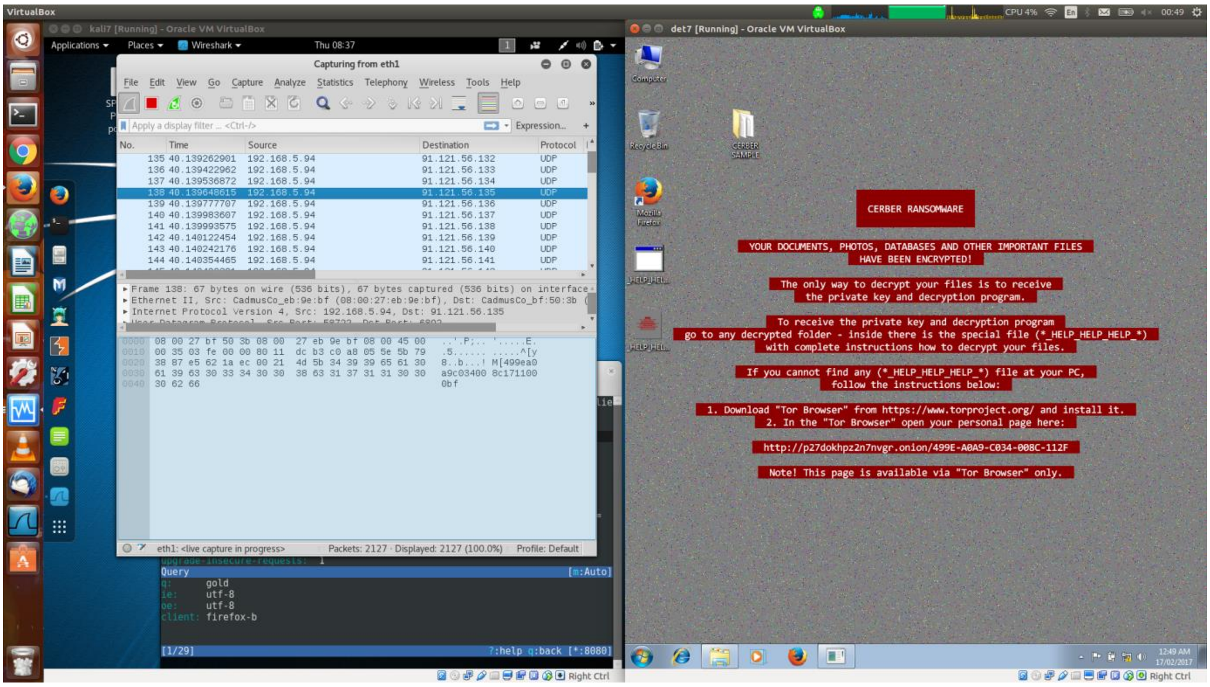
http://p27dokhpz2n7nvgr.1fqwek.top/499E-A0A9-C034-008C-112F

http://p27dokhpz2n7nvgr.1eeb86.top/499E-A0A9-C034-008C-112F

http://p27dokhpz2n7nvgr.1lt2pn.top/499E-A0A9-C034-008C-112F

http://p27dokhpz2n7nvgr.15jznv.top/499E-A0A9-C034-008C-112F

If this page cannot be opened, click here to get a new address of your personal page



```
No.  Time           Source         Destination     Protocol
 135 40.139262901   192.168.5.94   91.121.56.132   UDP
 136 40.139422962   192.168.5.94   91.121.56.133   UDP
 137 40.139536872   192.168.5.94   91.121.56.134   UDP
 138 40.139648615   192.168.5.94   91.121.56.135   UDP
 139 40.139777707   192.168.5.94   91.121.56.136   UDP
 140 40.139983607   192.168.5.94   91.121.56.137   UDP
 141 40.139993575   192.168.5.94   91.121.56.138   UDP
 142 40.140122454   192.168.5.94   91.121.56.139   UDP
 143 40.140242176   192.168.5.94   91.121.56.140   UDP
 144 40.140354465   192.168.5.94   91.121.56.141   UDP

▸ Frame 138: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface
▸ Ethernet II, Src: CadmusCo_eb:9e:bf (08:00:27:eb:9e:bf), Dst: CadmusCo_bf:50:3b (
▸ Internet Protocol Version 4, Src: 192.168.5.94, Dst: 91.121.56.135

0000  08 00 27 bf 50 3b 08 00  27 eb 9e bf 08 00 45 00   ..'.P;.. '.....E.
0010  00 35 03 fe 00 00 80 11  dc b3 c0 a8 05 5e 5b 79   .5...... .....^[y
0020  38 87 e5 62 1a ec 00 21  4d 5b 34 39 39 65 61 30   8..b...! M[499ea0
0030  61 39 63 30 33 34 30 30  38 63 31 37 31 31 30 30   a9c03400 8c171100
0040  30 62 66                                           0bf

eth1: <live capture in progress>   Packets: 2127 · Displayed: 2127 (100.0%)   Profile: Default
```

```
Query                                                        [m:Auto]
q:      gold
ie:     utf-8
oe:     utf-8
client: firefox-b

[1/29]                                     ?:help q:back [*:8080]
```

CERBER RANSOMWARE

YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES
HAVE BEEN ENCRYPTED!

The only way to decrypt your files is to receive
the private key and decryption program.

To receive the private key and decryption program
go to any decrypted folder - inside there is the special file (*_HELP_HELP_HELP_*)
with complete instructions how to decrypt your files.

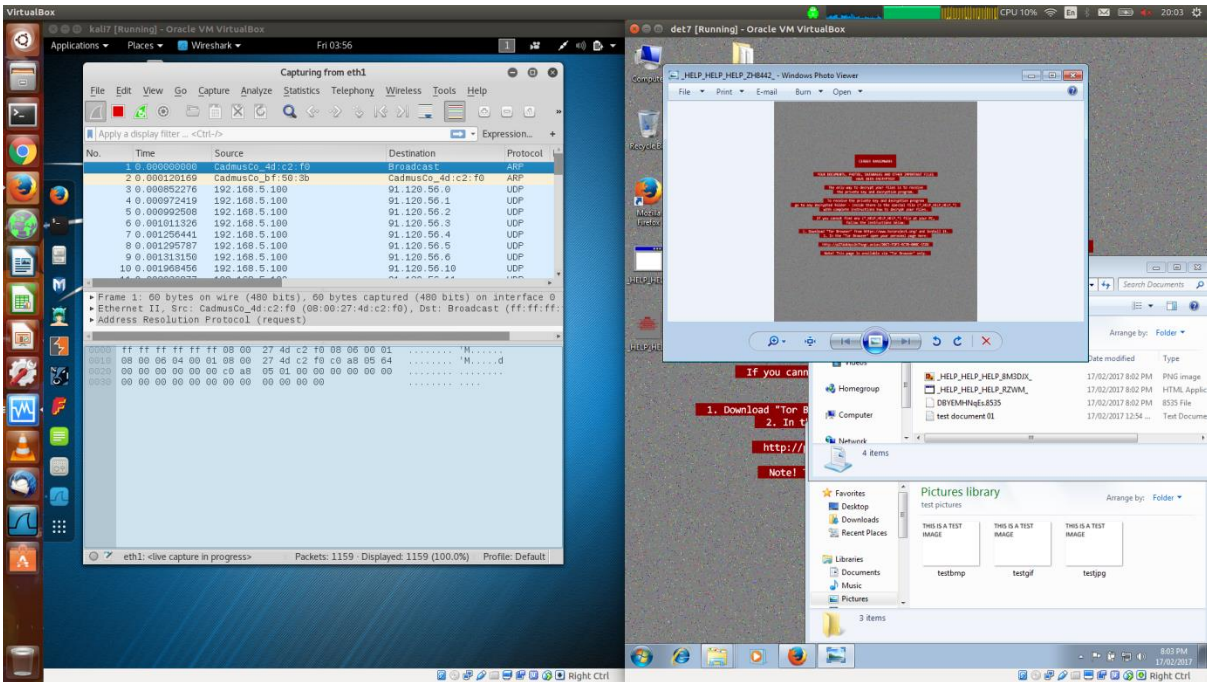
If you cannot find any (*_HELP_HELP_HELP_*) file at your PC,
follow the instructions below:

1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:

http://p27dokhpz2n7nvgr.onion/499E-A0A9-C034-008C-112F

Note! This page is available via "Tor Browser" only.

-
- Post execution showing the desktop changed to the ransom demand.

- 

```
No.  Time         Source              Destination          Protocol
   1 0.000000000  CadmusCo_4d:c2:f0   Broadcast            ARP
   2 0.000120169  CadmusCo_bf:50:3b   CadmusCo_4d:c2:f0    ARP
   3 0.000852276  192.168.5.100       91.120.56.0          UDP
   4 0.000972419  192.168.5.100       91.120.56.1          UDP
   5 0.000992508  192.168.5.100       91.120.56.2          UDP
   6 0.001011326  192.168.5.100       91.120.56.3          UDP
   7 0.001256441  192.168.5.100       91.120.56.4          UDP
   8 0.001295787  192.168.5.100       91.120.56.5          UDP
   9 0.001313150  192.168.5.100       91.120.56.6          UDP
  10 0.001968456  192.168.5.100       91.120.56.10         UDP

▸ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: CadmusCo_4d:c2:f0 (08:00:27:4d:c2:f0), Dst: Broadcast (ff:ff:ff:
▸ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 08 00  27 4d c2 f0 08 06 00 01   ........ 'M......
0010  08 00 06 04 00 01 08 00  27 4d c2 f0 c0 a8 05 64   ........ 'M.....d
0020  00 00 00 00 00 00 c0 a8  05 01 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....

eth1: <live capture in progress>    Packets: 1159 · Displayed: 1159 (100.0%)    Profile: Default
```

Name	Date modified	Type
_HELP_HELP_HELP_8M3DJX_	17/02/2017 8:02 PM	PNG image
_HELP_HELP_HELP_RZWM_	17/02/2017 8:02 PM	HTML Applic
DBYEMHNqEs.8535	17/02/2017 8:02 PM	8535 File
test document 01	17/02/2017 12:54 ...	Text Docume

- Post execution I can see the word document is scrambled, text document and image files appeared and opened fine.

Cuckoo analysis showed the payload executable running multiple processes.

1st Process phase 1 (2460)-

  - I noted a lot of python scripting with this process
  - A lot of inspection of .lnk filetypes.
  - This process appears to drop a lot of the PNG HELP_HELP files as shown above
  - It also writes .py (python) files.

1st Process phase 2 (2460)–

  - I noted a lot of inspection of .ini filetypes
  - This process appears to drop .dll files

2nd Process phase 3 (3004)–

  - Targets registry reads and accesses a lot of keys

1st Process phase 4 (2460)–

  - Targets registry making a number of changes

2nd process phase 5 (3004)-

  - Still targeting registry accessing an reading large number of keys.

1st Process phase 6 (2460)-

  - Registry – Mutexes around speech and voice tokens

2nd process phase 7 (3004)-

- Conducts cleanup using taskkill process.

1st process phase 8 (2460)-

- Creates windows directories and enumerates a large number od directory entries.

2nd process phase 9 (3004)-

- Creates group of appdata directories
- Enumerates a group of windows directories.

1st process phase 10 (2460)-

- Creates desktop drops for help files
- Loads large number of .dll filetypes

2nd process phase 11 (3004)-

- Drops payload executable to appdata local temp.
- Launches group of .dll's

Cerber appears designed for ease of use and currently is been seen trialled with differing delivery methods.

Thankyou

MBYX