CryptoWall

DNS

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

(LAYER: 4)
s_port: 62520 |d_port: 53 |len=53
    C7 9E 01 00 00 01 00 00 00 00 00 00 0D 73 75 70        .............sup
    65 72 63 72 61 76 69 6E 67 73 03 63 6F 6D 00 00        ercravings.com..
    01 00 01                                               ...
```

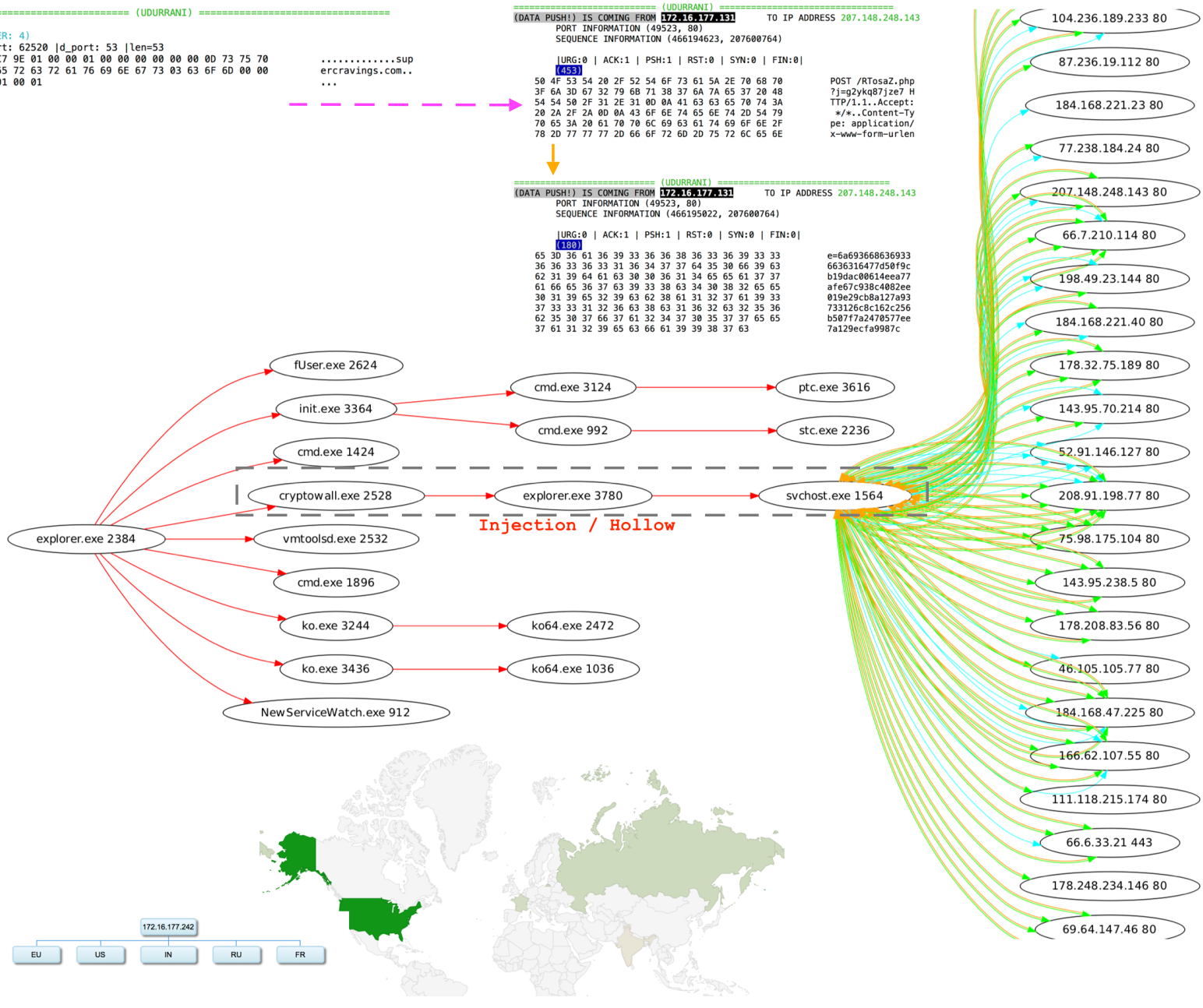
TCP

```
========================== (UDURRANI) ==============================
(DATA PUSH!) IS COMING FROM 172.16.177.131      TO IP ADDRESS 207.148.248.143
        PORT INFORMATION (49523, 80)
        SEQUENCE INFORMATION (466194623, 207600764)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (453)
    50 4F 53 54 20 2F 52 54 6F 73 61 5A 2E 70 68 70        POST /RTosaZ.php
    3F 6A 3D 67 32 79 6B 71 38 37 6A 7A 65 37 20 48        ?j=g2ykq87jze7 H
    54 54 50 2F 31 2E 31 0D 0A 41 63 63 65 70 74 3A        TTP/1.1..Accept:
    20 2A 2F 2A 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79         */*..Content-Ty
    70 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F        pe: application/
    78 2D 77 77 77 2D 66 6F 72 6D 2D 75 72 6C 65 6E        x-www-form-urlen

========================== (UDURRANI) ==============================
(DATA PUSH!) IS COMING FROM 172.16.177.131      TO IP ADDRESS 207.148.248.143
        PORT INFORMATION (49523, 80)
        SEQUENCE INFORMATION (466195022, 207600764)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (180)
    65 3D 36 61 36 39 33 36 36 38 36 33 36 39 33 33        e=6a693668636933
    36 36 33 36 33 31 36 34 37 37 64 35 30 66 39 63        6636316477d50f9c
    62 31 39 64 61 63 30 30 36 31 34 65 65 61 37 37        b19dac00614eea77
    61 66 65 36 37 63 39 33 38 63 34 30 38 32 65 65        afe67c938c4082ee
    30 31 39 65 32 39 63 62 38 61 31 32 37 61 39 33        019e29cb8a127a93
    37 33 33 31 32 36 63 38 63 31 36 32 63 32 35 36        733126c8c162c256
    62 35 30 37 66 37 61 32 34 37 30 35 37 37 65 65        b507f7a2470577ee
    37 61 31 32 39 65 63 66 61 39 39 38 37 63              7a129ecfa9987c
```



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

(LAYER: 4)
s_port: 59647 |d_port: 53 |len=53

DOMAIN

```
    82 1E 01 00 00 01 00 00 00 00 00 00 03 77 77 77        .............www
    06 6D 79 73 68 6F 70 02 6C 6B 00 00 01 00 01           .myshop.lk.....
```

(LAYER: 4)
s_port: 60623 |d_port: 53 |len=53

DOMAIN

```
    6F 08 01 00 00 01 00 00 00 00 00 00 08 61 64 72        o.............adr
    69 76 65 36 32 03 63 6F 6D 00 00 01 00 01              ive62.com.....
```

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

(LAYER: 4)
s_port: 61067 |d_port: 53 |len=53

DOMAIN

```
    68 6B 01 00 00 01 00 00 00 00 00 00 0C 68 74 74        hk...........htt
    74 68 61 6E 67 6C 6F 6E 67 03 63 6F 6D 00 00 01        thanglong.com...
    00 01                                                  ..
```

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

(LAYER: 4)
s_port: 59504 |d_port: 53 |len=53

DOMAIN

```
    F3 36 01 00 00 01 00 00 00 00 00 00 14 63 68 61        .6...........cha
    6D 70 61 67 6E 65 66 72 61 6D 65 6F 66 6D 69 6E        mpagneframeofmin
    64 03 63 6F 6D 00 00 01 00 01                          d.com.....
```

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

(LAYER: 4)
s_port: 51027 |d_port: 53 |len=53

DOMAIN

```
    03 5E 01 00 00 01 00 00 00 00 00 00 0D 61 64 63        .^...........adc
    63 6F 6E 73 75 6C 74 69 6E 67 03 6E 65 74 00 00        consulting.net..
    01 00 01                                               ...
```

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

(LAYER: 4)
s_port: 64908 |d_port: 53 |len=53

DOMAIN

```
    A1 60 01 00 00 01 00 00 00 00 00 00 14 72 6F 79        .`...........roy
    61 6C 73 62 6F 6F 73 74 65 72 73 67 62 62 61 6C        alsboostersgbbal
    6C 03 63 6F 6D 00 00 01 00 01                          l.com.....
```

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

(LAYER: 4)
s_port: 62520 |d_port: 53 |len=53

DOMAIN

```
    C7 9E 01 00 00 01 00 00 00 00 00 00 0D 73 75 70          .............sup
    65 72 63 72 61 76 69 6E 67 73 03 63 6F 6D 00 00          ercravings.com..
    01 00 01                                                 ...
```

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

(LAYER: 4)
s_port: 55856 |d_port: 53 |len=53

DOMAIN

```
    E5 41 01 00 00 01 00 00 00 00 00 00 06 6D 79 73          .A...........mys
    68 6F 70 02 6C 6B 00 00 01 00 01                         hop.lk.....
```

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

(LAYER: 4)
s_port: 53170 |d_port: 53 |len=53

DOMAIN

```
    EE CF 01 00 00 01 00 00 00 00 00 00 11 67 65 72          .............ger
    62 65 72 69 6E 73 72 65 66 65 72 72 61 6C 03 63          berinsreferral.c
    6F 6D 00 00 01 00 01                                     om.....
```

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

(LAYER: 4)
s_port: 63503 |d_port: 53 |len=53

DOMAIN

```
    D7 BE 01 00 00 01 00 00 00 00 00 00 09 6C 65 78          .............lex
    73 63 68 65 65 70 03 63 6F 6D 00 00 01 00 01             scheep.com.....
```

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

(LAYER: 4)
s_port: 56369 |d_port: 53 |len=53

DOMAIN

```
    30 F6 01 00 00 01 00 00 00 00 00 00 08 70 61 72          0............par
    73 69 6D 61 6A 03 63 6F 6D 00 00 01 00 01                simaj.com.....
```

```
(LAYER: 4)                                                          DOMAIN
s_port: 63077 |d_port: 53 |len=53
    CC 57 01 00 00 01 00 00 00 00 00 00 06 6B 73 30        .W..........ks0
    34 30 37 03 63 6F 6D 00 00 01 00 01                    407.com.....


(LAYER: 4)
s_port: 53 |d_port: 62213 |len=62213
    1D DE 81 80 00 01 00 01 00 00 00 00 0E 73 74 77        ...?.........stw
============================ (UDURRANI) ================================

(LAYER: 4)                                                          DOMAIN
s_port: 60435 |d_port: 53 |len=53
    EF 32 01 00 00 01 00 00 00 00 00 00 09 74 68 65        .2...........the
    67 69 6E 67 6F 64 03 63 6F 6D 00 00 01 00 01           gingod.com.....


 77 77 2E 70 61 72 73 69 6D 61 6A 2E 63 6F 6D 2F        ww.parsimaj.com/
 25 64 39 25 62 65 25 64 38 25 62 31 25 64 39 25        %d9%be%d8%b1%d9%
 38 38 25 64 61 25 39 38 25 64 39 25 38 37 2D 25        88%da%98%d9%87-%
 64 39 25 38 37 25 64 38 25 61 37 25 64 62 25 38        d9%87%d8%a7%db%8
 63 2D 25 64 38 25 61 37 25 64 38 25 61 63 25 64        c-%d8%a7%d8%ac%d
 38 25 62 31 25 64 38 25 61 37 2D 25 64 38 25 62        8%b1%d8%a7-%d8%b
 34 25 64 38 25 61 66 25 64 39 25 38 37 2D 25 64        4%d8%af%d9%87-%d
 39 25 38 36 25 64 39 25 38 35 25 64 38 25 61 37        9%86%d9%85%d8%a7
 2D 25 64 62 25 62 39 25 64 62 25 62 34 2D 25 64        -%db%b9%db%b4-%d
 62 25 62 39 25 64 62 25 62 35 2F 25 64 38 25 61        b%b9%db%b5/%d8%a
 37 25 64 38 25 61 63 25 64 38 25 62 31 25 64 38        7%d8%ac%d8%b1%d8
 25 61 37 25 64 62 25 38 63 2D 25 64 38 25 61 61        %a7%db%8c-%d8%aa
 25 64 38 25 61 37 25 64 38 25 61 38 25 64 39 25        %d8%a7%d8%a8%d9%
 38 34 25 64 39 25 38 38 2D 25 64 61 25 61 39 25        84%d9%88-%da%a9%
 64 38 25 61 37 25 64 39 25 38 35 25 64 39 25 62        d8%a7%d9%85%d9%b
 65 25 64 39 25 38 38 25 64 38 25 62 32 25 64 62        e%d9%88%d8%b2%db
 25 38 63 25 64 38 25 61 61 2D 25 64 39 25 38 32        %8c%d8%aa-%d9%82
 25 64 38 25 62 31 25 64 62 25 38 63 25 64 38 25        %d8%b1%db%8c%d8%
```

IP Addresses

Process is trying to communicate but no response

Process is communicating

104.236.189.233 80
104.236.189.233 80
207.148.248.143 80
87.236.19.112 80
66.7.210.114 80
184.168.221.40 80
178.32.75.189 80
184.168.221.23 80
143.95.70.214 80
52.91.146.127 80
208.91.198.77 80
75.98.175.104 80
143.95.238.5 80
66.7.210.114 80
184.168.47.225 80
184.168.47.225 80
166.62.107.55 80
77.238.184.24 80
66.6.33.21 443
208.91.198.77 80
69.64.147.46 80
69.64.147.46 80
104.236.189.233 80
198.49.23.144 80
104.27.138.20 80
178.32.75.189 80
143.95.70.214 80
52.91.146.127 80
208.91.198.77 80
208.91.198.77 80
75.98.175.104 80
143.95.238.5 80
184.168.47.225 80
184.168.47.225 80
166.62.107.55 80
166.62.107.55 80

69.64.147.46 80
104.236.189.233 80
104.236.189.233 80
207.148.248.143 80
198.49.23.144 80
184.168.221.40 80
178.32.75.189 80
143.95.70.214 80
52.91.146.127 80
208.91.198.77 80
75.98.175.104 80
143.95.238.5 80
66.7.210.114 80
46.105.105.77 80
184.168.47.225 80
166.62.107.55 80
166.62.107.55 80
66.6.33.21 443
178.208.83.56 80
208.91.198.77 80
69.64.147.46 80
207.148.248.143 80
66.7.210.114 80
198.49.23.144 80
184.168.221.40 80
178.32.75.189 80
143.95.70.214 80
52.91.146.127 80
208.91.198.77 80
75.98.175.104 80
143.95.238.5 80
178.208.83.56 80
66.7.210.114 80
46.105.105.77 80
184.168.47.225 80
184.168.47.225 80
166.62.107.55 80
111.118.215.174 80
66.6.33.21 443
178.208.83.56 80
178.248.234.146 80
208.91.198.77 80

LOADED MODULES:

```
C:\Windows\syswow64\svchost.exe      [ 0x00330000 ]
C:\Windows\SysWOW64\ntdll.dll     [ 0x773F0000 ]
C:\Windows\syswow64\kernel32.dll     [ 0x75170000 ]
C:\Windows\syswow64\KERNELBASE.dll      [ 0x75270000 ]
C:\Windows\syswow64\msvcrt.dll     [ 0x76920000 ]
C:\Windows\SysWOW64\sechost.dll     [ 0x76BF0000 ]
C:\Windows\syswow64\RPCRT4.dll     [ 0x76530000 ]
C:\Windows\syswow64\SspiCli.dll     [ 0x74F60000 ]
C:\Windows\syswow64\CRYPTBASE.dll      [ 0x74F50000 ]
C:\Windows\syswow64\advapi32.dll     [ 0x769D0000 ]
C:\Windows\syswow64\user32.dll     [ 0x752C0000 ]
C:\Windows\syswow64\GDI32.dll     [ 0x76410000 ]
C:\Windows\syswow64\LPK.dll     [ 0x76260000 ]
C:\Windows\syswow64\USP10.dll     [ 0x76B50000 ]
C:\Windows\system32\IMM32.DLL     [ 0x753C0000 ]
C:\Windows\syswow64\MSCTF.dll     [ 0x76A80000 ]
C:\Windows\syswow64\ole32.dll     [ 0x76620000 ]
C:\Windows\syswow64\wininet.dll     [ 0x76EF0000 ]
C:\Windows\syswow64\SHLWAPI.dll     [ 0x755B0000 ]
C:\Windows\syswow64\Normaliz.dll     [ 0x773C0000 ]
C:\Windows\syswow64\urlmon.dll     [ 0x762D0000 ]
C:\Windows\syswow64\OLEAUT32.dll     [ 0x764A0000 ]
C:\Windows\syswow64\CRYPT32.dll     [ 0x74FC0000 ]
C:\Windows\syswow64\MSASN1.dll     [ 0x76A70000 ]
C:\Windows\syswow64\iertutil.dll     [ 0x76C10000 ]
C:\Windows\syswow64\CRYPTSP.dll     [ 0x748C0000 ]
C:\Windows\system32\rsaenh.dll     [ 0x74880000 ]
C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\c
omctl32.dll     [ 0x748F0000 ]
C:\Windows\syswow64\SHELL32.dll     [ 0x75610000 ]
C:\Windows\syswow64\profapi.dll     [ 0x748E0000 ]
C:\Windows\syswow64\ws2_32.DLL     [ 0x76280000 ]
C:\Windows\syswow64\NSI.dll     [ 0x762C0000 ]
C:\Windows\syswow64\dnsapi.DLL     [ 0x73D00000 ]
C:\Windows\syswow64\iphlpapi.DLL     [ 0x74D50000 ]
C:\Windows\syswow64\WINNSI.DLL     [ 0x74D80000 ]
C:\Windows\syswow64\RASAPI32.dll     [ 0x72F30000 ]
C:\Windows\syswow64\rasman.dll     [ 0x73290000 ]
C:\Windows\syswow64\rtutils.dll     [ 0x73B10000 ]
C:\Windows\syswow64\sensapi.dll     [ 0x73A40000 ]
C:\Windows\system32\NLAapi.dll     [ 0x73780000 ]
C:\Windows\syswow64\rasadhlp.dll     [ 0x73280000 ]
```

```
C:\Windows\System32\mswsock.dll      [ 0x73BA0000 ]
C:\Windows\System32\winrnr.dll      [ 0x73270000 ]
C:\Windows\system32\napinsp.dll      [ 0x731A0000 ]
C:\Windows\system32\pnrpnsp.dll      [ 0x730B0000 ]
C:\Windows\system32\wshbth.dll      [ 0x73180000 ]
C:\Windows\System32\wshtcpip.dll      [ 0x73C10000 ]
C:\Windows\System32\wship6.dll      [ 0x730A0000 ]
C:\Windows\System32\fwpuclnt.dll      [ 0x72E30000 ]
C:\Windows\syswow64\CLBCatQ.DLL      [ 0x750E0000 ]
C:\Windows\System32\netprofm.dll      [ 0x728D0000 ]
C:\Windows\syswow64\RpcRtRemote.dll      [ 0x73090000 ]
C:\Windows\System32\npmproxy.dll      [ 0x73080000 ]
C:\Windows\syswow64\ntmarta.dll      [ 0x74850000 ]
C:\Windows\syswow64\WLDAP32.dll      [ 0x76E10000 ]
C:\Windows\syswow64\VERSION.dll      [ 0x73190000 ]
C:\Windows\syswow64\USERENV.dll      [ 0x73BE0000 ]
C:\Windows\syswow64\wintrust.dll      [ 0x75580000 ]
C:\Windows\syswow64\schannel.DLL      [ 0x73C70000 ]
C:\Windows\syswow64\credssp.dll      [ 0x728B0000 ]
C:\Windows\syswow64\secur32.dll      [ 0x728A0000 ]
C:\Windows\syswow64\ncrypt.dll      [ 0x72860000 ]
C:\Windows\syswow64\bcrypt.dll      [ 0x73A90000 ]
C:\Windows\SysWOW64\bcryptprimitives.dll      [ 0x73A50000 ]
C:\Windows\syswow64\GPAPI.dll      [ 0x72840000 ]
C:\Windows\syswow64\cryptnet.dll      [ 0x72820000 ]
C:\Windows\syswow64\Cabinet.dll      [ 0x74330000 ]
C:\Windows\syswow64\DEVRTL.dll      [ 0x74320000 ]
C:\Windows\syswow64\peerdist.dll      [ 0x74C20000 ]
C:\Windows\syswow64\AUTHZ.dll      [ 0x74C60000 ]
```