Backbone Network Security Visibility In Practice

Yang Xu

Twitter: @xuy1202

Network Security Research Lab, Qihoo 360

http://netlab.360.com/

Our Team, Our Goal

Thread Research, Security Basic Data, See More:

- DDoS monitoring
- Scanner tracking
- Bot-Net tracking
- DGA cracking
- Fast-flux
- Phishing
- ……

WHY

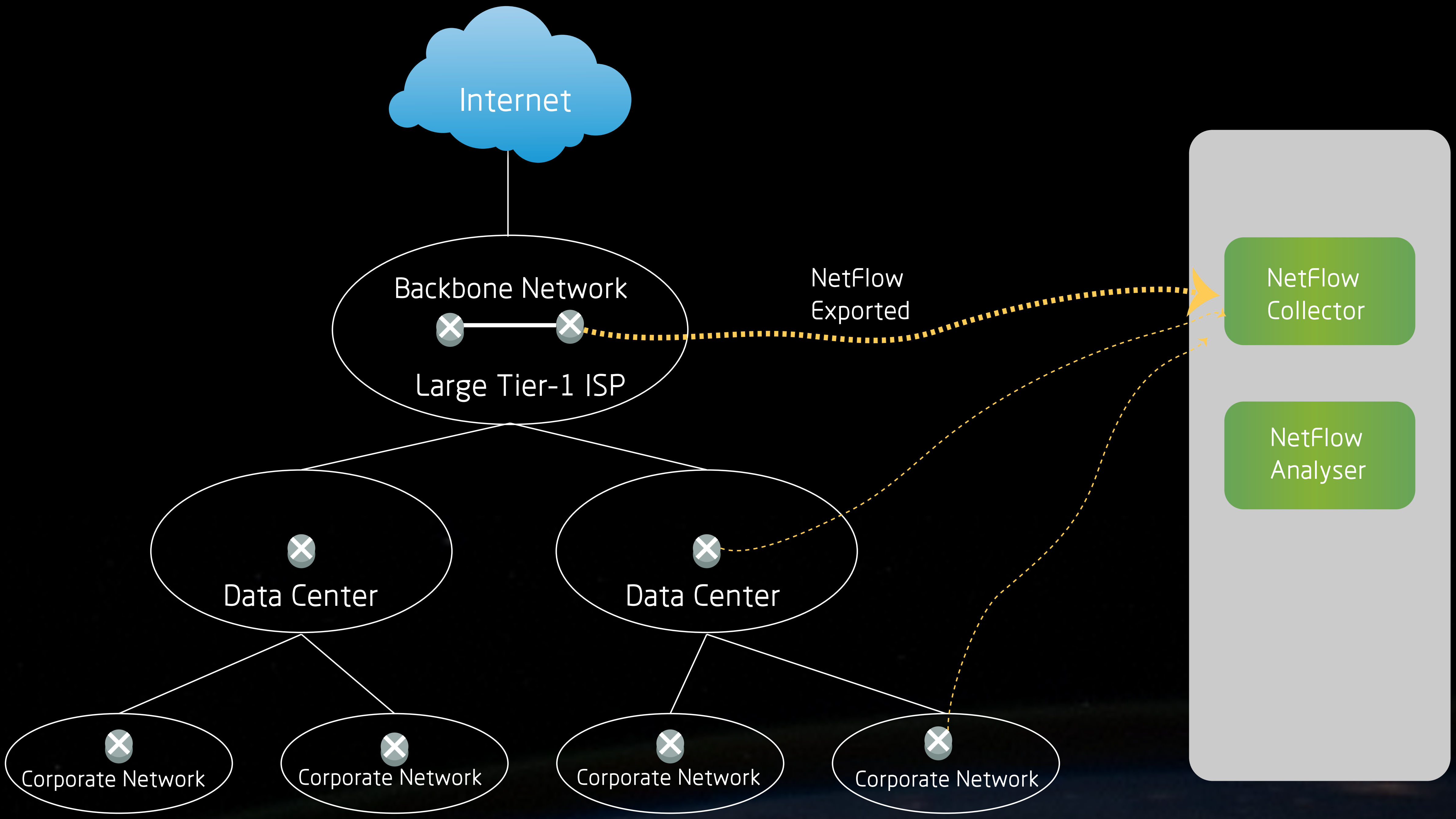
“We are living in the Dark Ages of security. We cling to outmoded world views and rely on tools and tactics from the past, and yet we are surprised to find ourselves living in an era of chaos and violence. We must cast off the past and enter an Age of Enlightenment by pursuing greater visibility into and understanding of our digital world.”

——RSA2015 USA, Escaping Security’ s Dark Ages, President Amit

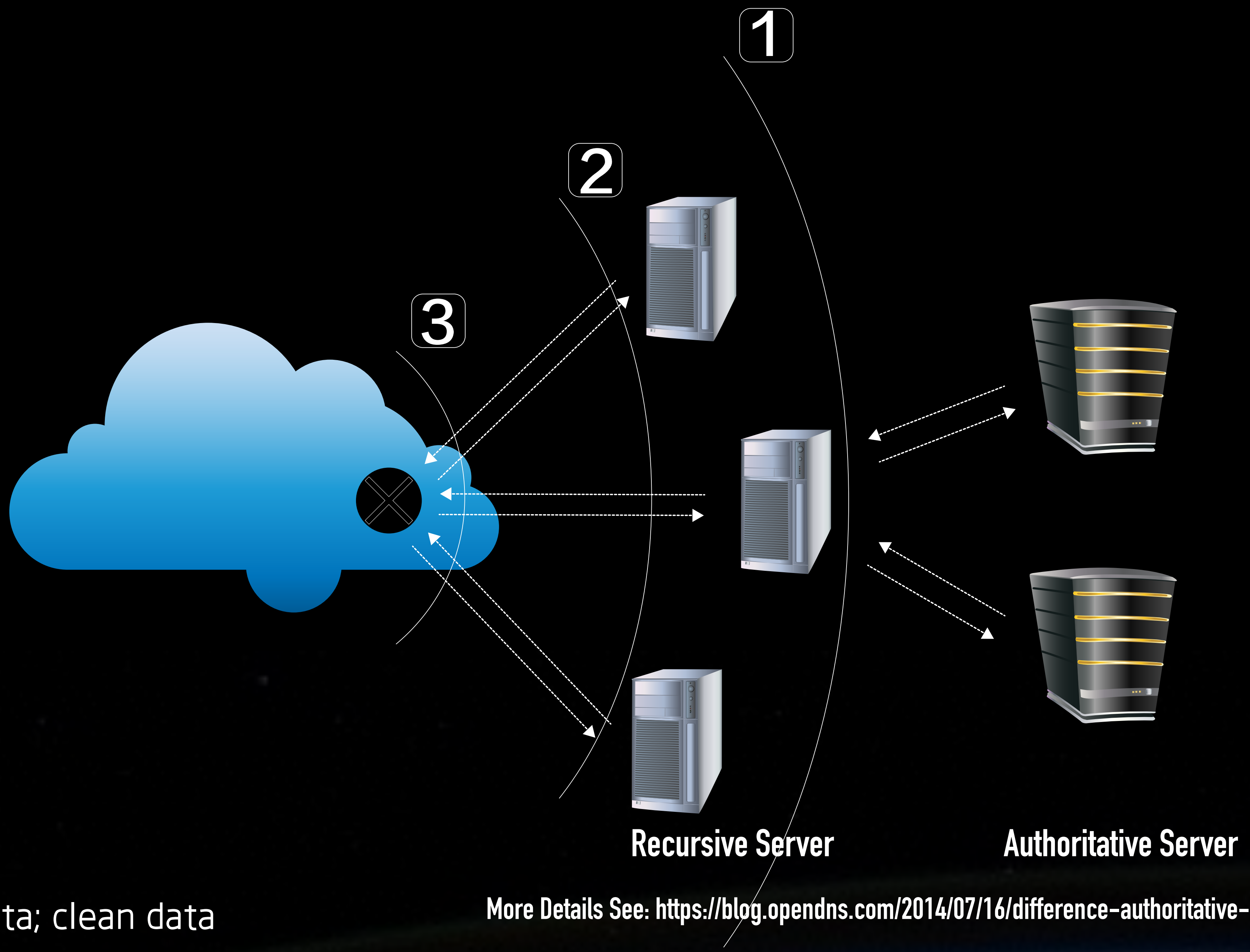
Security visibility leads to threat intelligence

Know what happens on the internet, know our potential enemy

NetFlow Collecting



PDNS Collecting



More Details See: https://blog.opendns.com/2014/07/16/difference-authoritative-recursive-dns-nameservers/

1: small data; clean data

2: with client info; know query to me, NO know query to others; src port; query transaction id

3: client focused perspective, richer info

Dealing With BIIIG Data

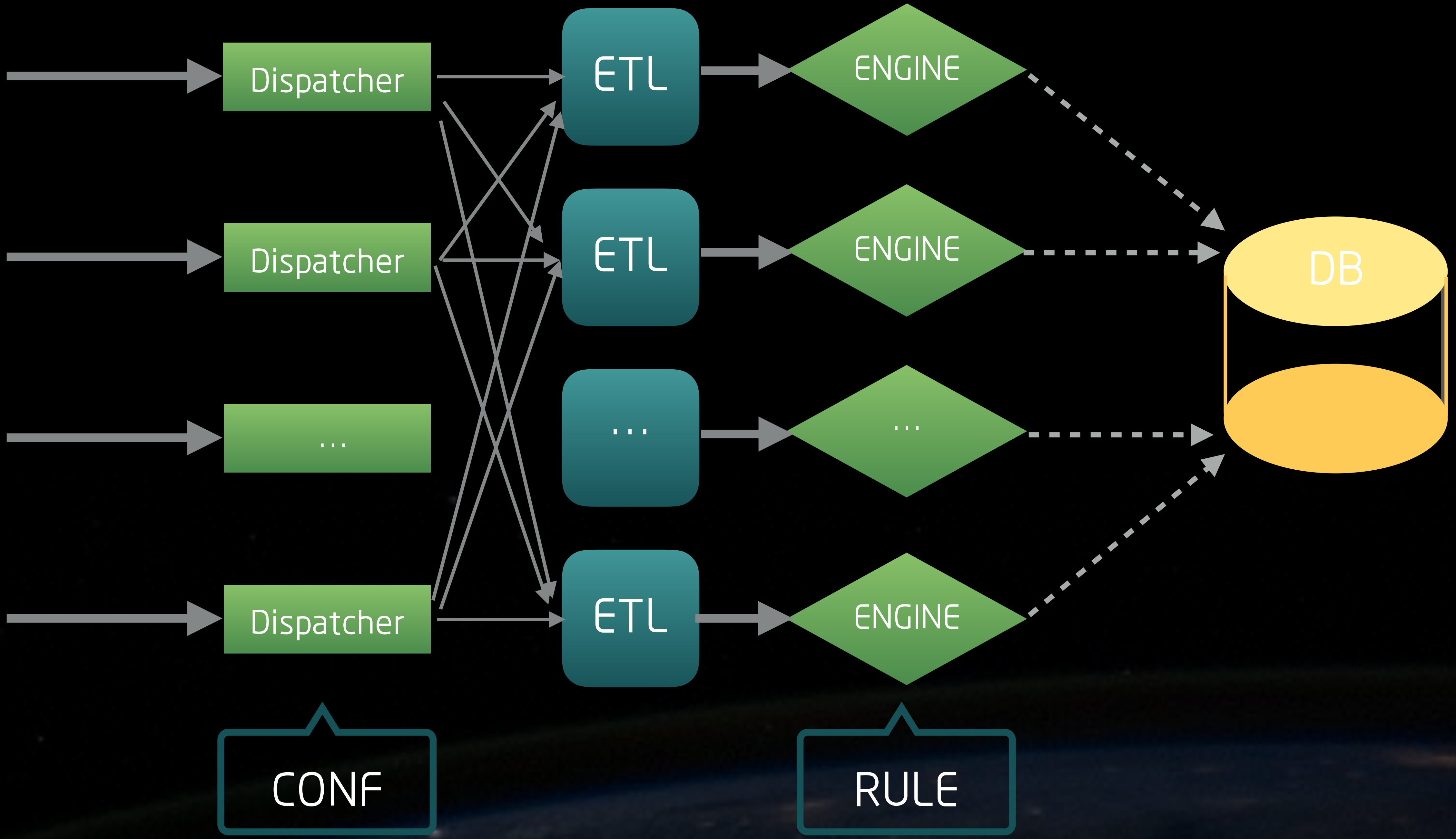
NetFlow - 30B/day on average, 3M/second at peak

PDNS - 300B/day on average, 5M/second at peak

- All processing in Memory
- Developed in pure C++ with ZMQ as MQ
- Horizontal Partitioning
- Tiered Sampling, the earlier the better

A Protocol for Dying: http://hintjens.com/blog:115

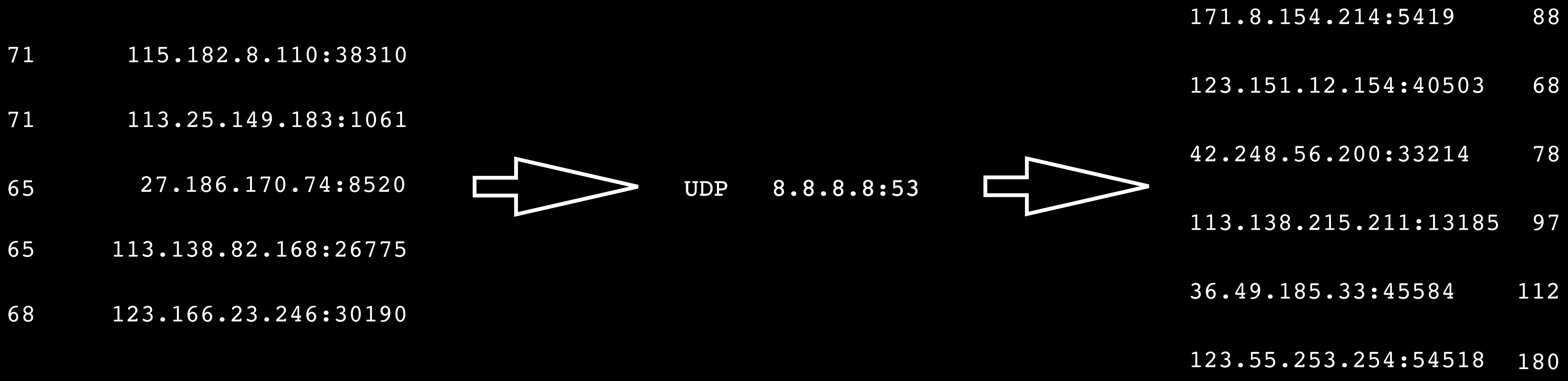
Dealing With BIIIG Data



Data Modeling

```
Date flow start      Duration   Porto   Src IP Addr:Port                 Dst IP Addr:Port        Flags       Tos Packets Bytes
2016-09-18 19:12:49       0      UDP    8.8.8.8:53                 ->    171.8.154.214:5419      ......       180   1      88
2016-09-18 19:22:53       0      TCP    36.105.14.141:65100        ->    8.8.8.8:53              ....S.       0     1      60
2016-09-18 19:16:31       0      UDP    115.182.8.110:38310        ->    8.8.8.8:53              ......       0     1      71
2016-09-18 19:14:08       0      TCP    61.185.165.150:44872       ->    8.8.8.8:53              .A....       0     1      52
2016-09-18 19:11:30       0      UDP    8.8.8.8:53                 ->    123.151.12.154:40503    ......       180   1      68
2016-09-18 19:20:17       0      UDP    113.25.149.183:1061        ->    8.8.8.8:53              ......       0     1      71
2016-09-18 19:14:42       0      TCP    8.8.8.8:53                 ->    111.225.110.122:11731   .A..S.       180   1      60
2016-09-18 19:12:45       0      TCP    110.157.155.106:24049      ->    8.8.8.8:53              ....S.       0     1      60
2016-09-18 19:06:01       0      UDP    27.186.170.74:8520         ->    8.8.8.8:53              ......       0     1      65
2016-09-18 19:23:11       0      UDP    8.8.8.8:53                 ->    42.248.56.200:33214     ......       180   1      78
2016-09-18 19:02:26       0      UDP    8.8.8.8:53                 ->    113.138.215.211:13185   ......       180   1      97
2016-09-18 19:21:51       0      TCP    8.8.8.8:53                 ->    123.183.79.144:43047    .A..S.       180   1      64
2016-09-18 19:21:53       0      UDP    113.138.82.168:26775       ->    8.8.8.8:53              ......       0     1      65
2016-09-18 19:06:46       0      UDP    8.8.8.8:53                 ->    36.49.185.33:45584      ......       180   1      112
2016-09-18 19:00:30       0      UDP    8.8.8.8:53                 ->    123.55.253.254:54518    ......       180   1      180
2016-09-18 19:04:29       0      ICMP   8.8.8.8:0                  ->    101.251.1.127:0         ......       180   1      28
2016-09-18 19:22:18       0      UDP    123.166.23.246:30190       ->    8.8.8.8:53              ......       0     1      68
```

Data Modeling



```
71        115.182.8.110:38310
71        113.25.149.183:1061
65         27.186.170.74:8520
65       113.138.82.168:26775
68       123.166.23.246:30190
```

```
UDP    8.8.8.8:53
```

```
171.8.154.214:5419       88
123.151.12.154:40503     68
42.248.56.200:33214      78
113.138.215.211:13185    97
36.49.185.33:45584      112
123.55.253.254:54518    180
```

Data Modeling

Multi-Layer Net Pivot Model ~~MLNP~~

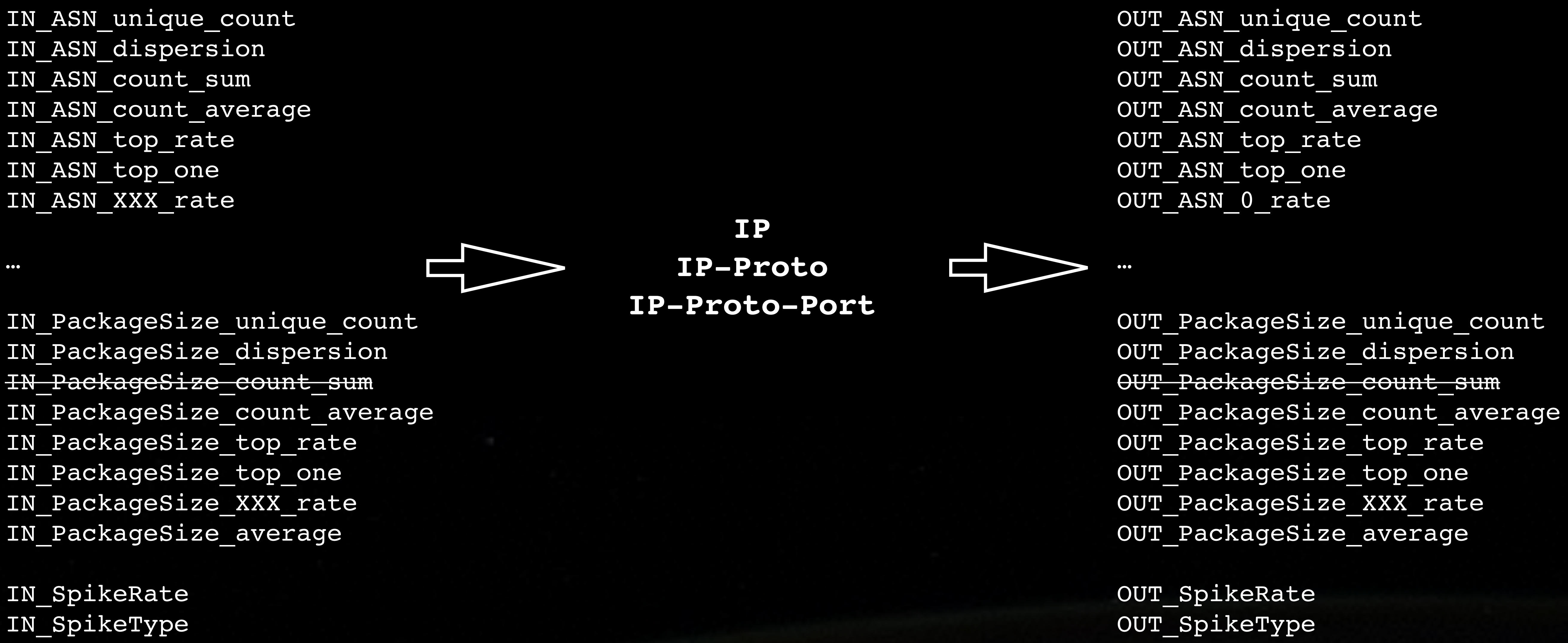
- Net Pivot: IN & OUT
- Multi-Layer: Drill-down & Roll-up

  IP / IP-Protocol / IP-Protocol-Port

Feature Matrix

DIR	Data Terms	Method
IN	{ASN: Count}	Map-length : unique_count
	{IP: Count}	Map-Dispersion : dispersion
	{Port: Count}	Value-Sum : count_sum
	{Peer(IP:Port): Count}	Value-Average : count_average
	{TcpFlags: Count}	Value-Top-Ratio : top_rate
OUT	{Duration: Count}	key-Top : top_one
	{Packages: Count}	key-Ratio : *_rate
	{PackageSize: count}	Key-Average : average
	Spike Type/Ratio	

Data Modeling



IN_ASN_unique_count
IN_ASN_dispersion
IN_ASN_count_sum
IN_ASN_count_average
IN_ASN_top_rate
IN_ASN_top_one
IN_ASN_XXX_rate

…

IN_PackageSize_unique_count
IN_PackageSize_dispersion
~~IN_PackageSize_count_sum~~
IN_PackageSize_count_average
IN_PackageSize_top_rate
IN_PackageSize_top_one
IN_PackageSize_XXX_rate
IN_PackageSize_average

IN_SpikeRate
IN_SpikeType

IP
IP-Proto
IP-Proto-Port

OUT_ASN_unique_count
OUT_ASN_dispersion
OUT_ASN_count_sum
OUT_ASN_count_average
OUT_ASN_top_rate
OUT_ASN_top_one
OUT_ASN_0_rate

…

OUT_PackageSize_unique_count
OUT_PackageSize_dispersion
~~OUT_PackageSize_count_sum~~
OUT_PackageSize_count_average
OUT_PackageSize_top_rate
OUT_PackageSize_top_one
OUT_PackageSize_XXX_rate
OUT_PackageSize_average

OUT_SpikeRate
OUT_SpikeType

Feature Choice

SYN Port Scanner

- Basic:

```
OUT_IP_dispersion       : scattered
OUT_Port_dispersion     : concentrated
OUT_TcpFlags_top_one    : SYN
OUT_TcpFlags_dispersion: concentrated
```

- “Bsides”:

```
OUT_IP/24_dispersion    : scattered
OUT_PackageSize_average: < 70
OUT_Duration_average    : 0
OUT_IP_count_average    : 1
```

Feature Choice

DRDoS Target

- Basic:

```
IN_SpikeRate                : high
IN_IP_dispersion            : scattered
IN_Port_dispersion          : concentrated
IN_Port_top_one             : [19,1900,53,123…]
```

- “Bsides”:

```
IN_Port_0_rate              : >0
IN_PackageSize_dispersion: concentrated
```

Feature Choice

What’s this?

- Basic:

```
OUT_SpikeRate                   : high
OUT_TcpFlags_dispersion         : concentrated
OUT_TcpFlags_top_one            : SYN+ACK
```

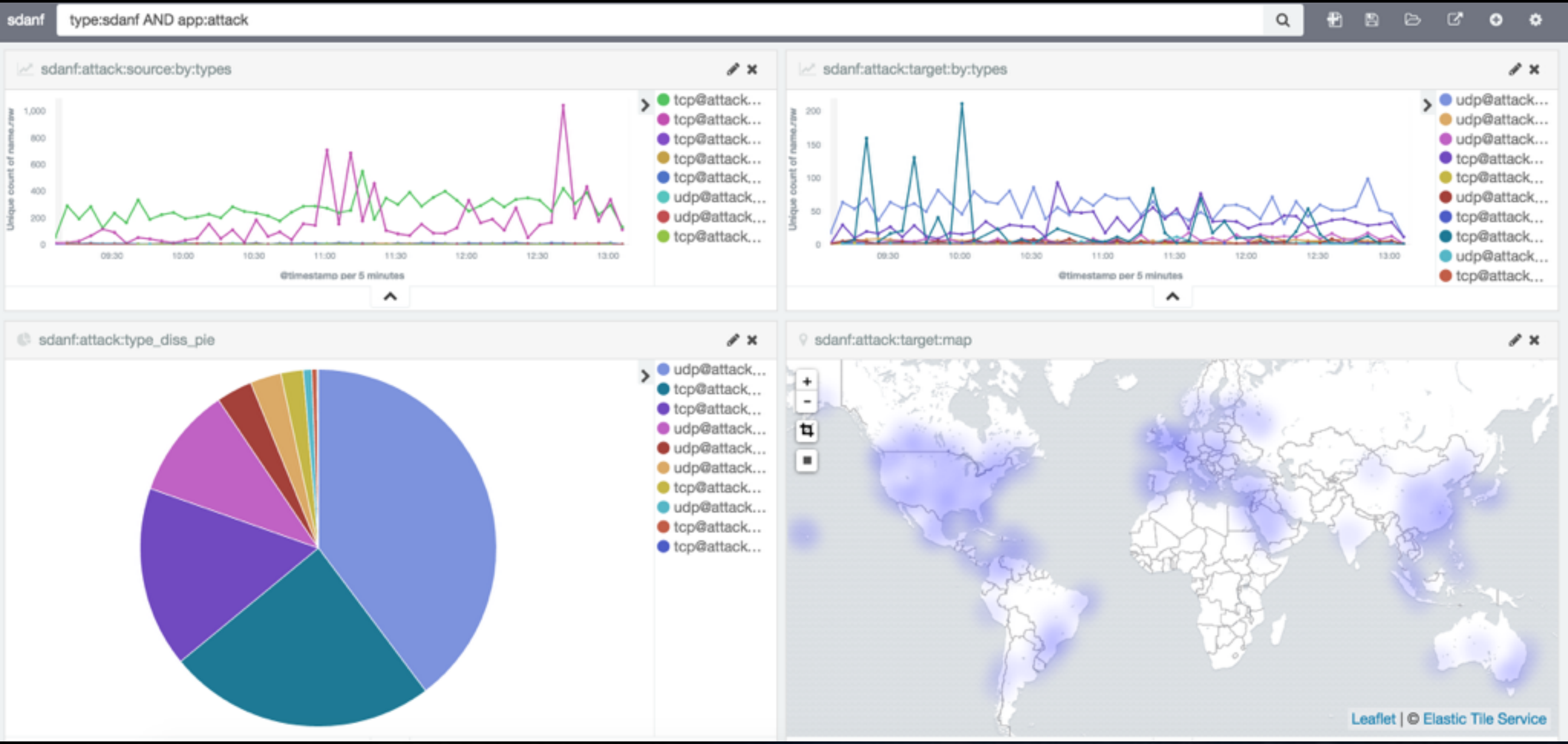
- “Bsides”:

  ?

“Bsides”

- MO: Manage Object
- Partial data
- ICMP as Side Indicator: false positive & false negative
- Integration with Third-party Data: PDNS, bot-net, honeypot
- weakness: like Slow Http Attack

What We Got



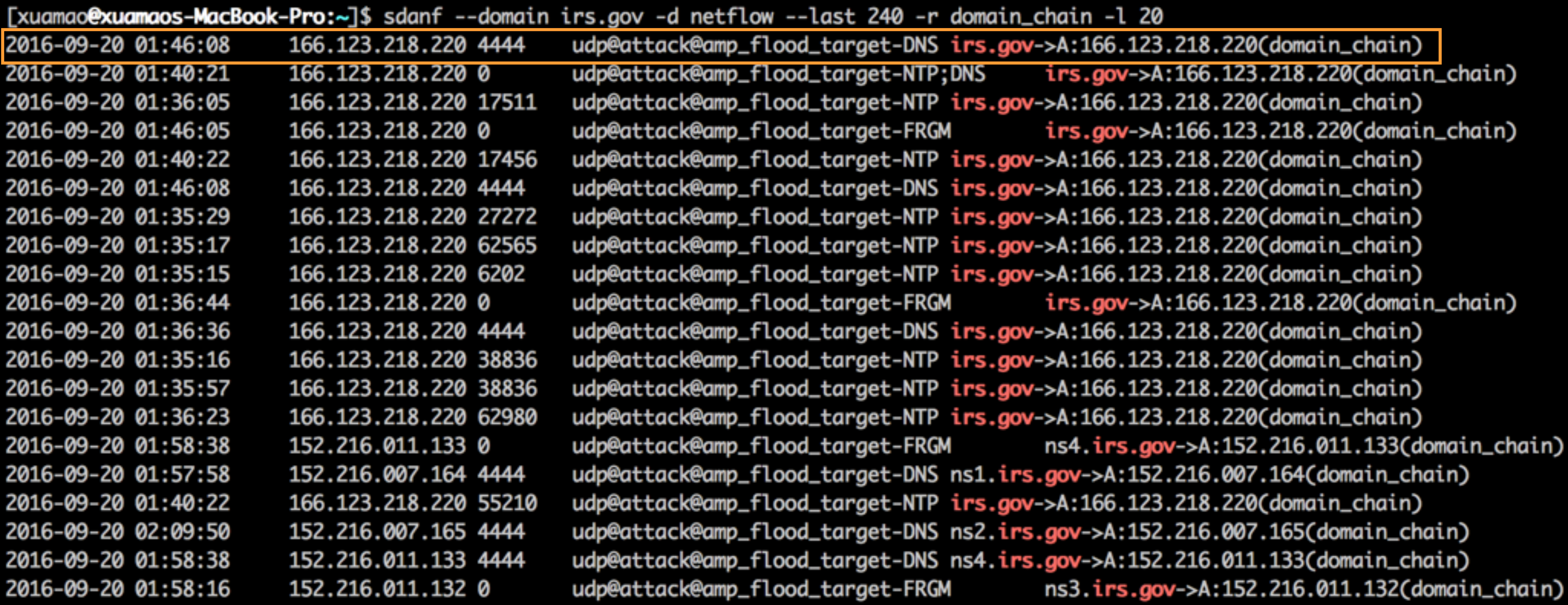
sdanf

type:sdanf AND app:attack

What We Got

PROFILE!

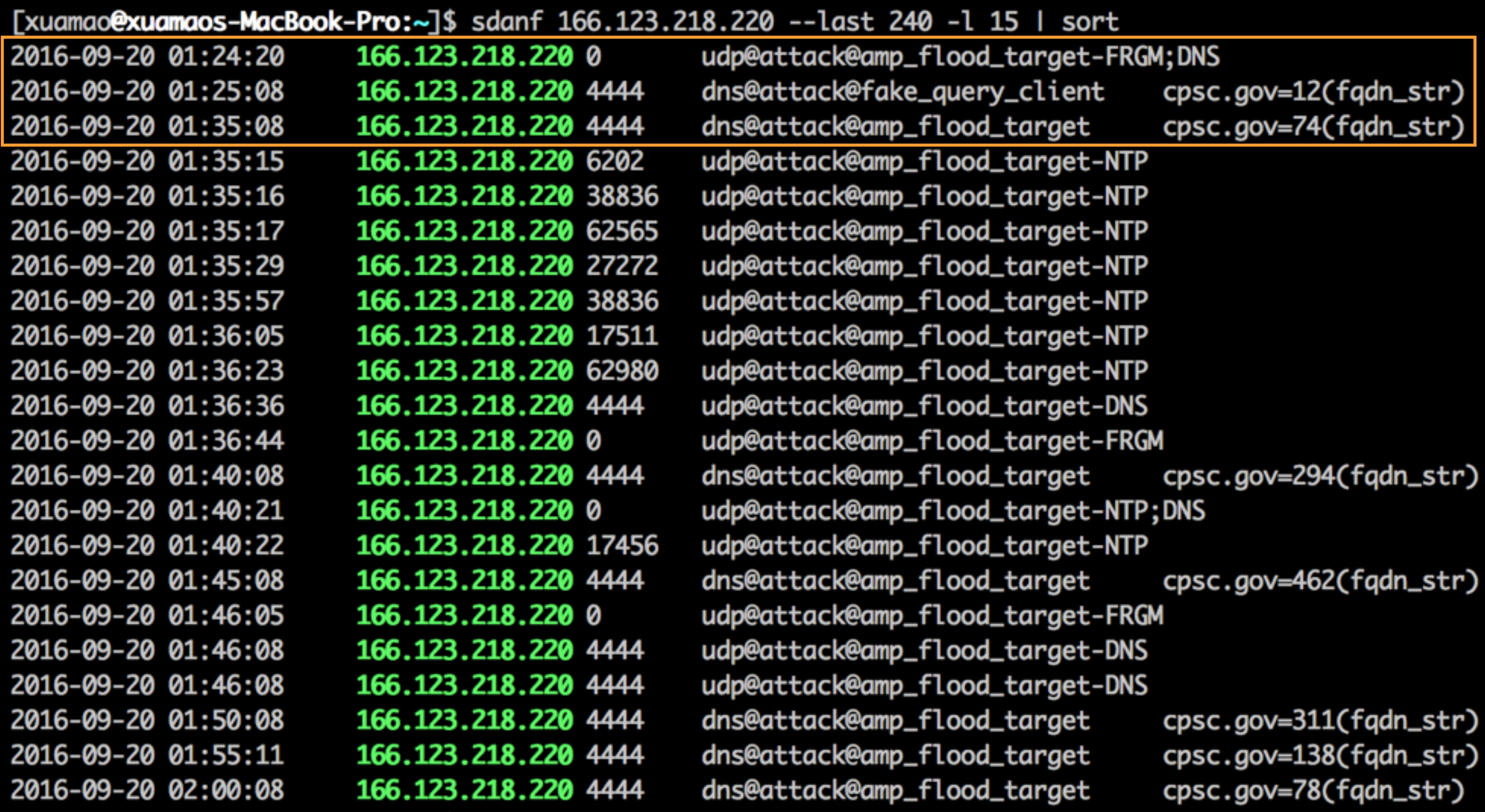
Case: irs.gov



```
[xuamao@xuamaos-MacBook-Pro:~]$ sdanf --domain irs.gov -d netflow --last 240 -r domain_chain -l 20
2016-09-20 01:46:08     166.123.218.220 4444     udp@attack@amp_flood_target-DNS irs.gov->A:166.123.218.220(domain_chain)
2016-09-20 01:40:21     166.123.218.220 0        udp@attack@amp_flood_target-NTP;DNS     irs.gov->A:166.123.218.220(domain_chain)
2016-09-20 01:36:05     166.123.218.220 17511    udp@attack@amp_flood_target-NTP irs.gov->A:166.123.218.220(domain_chain)
2016-09-20 01:46:05     166.123.218.220 0        udp@attack@amp_flood_target-FRGM        irs.gov->A:166.123.218.220(domain_chain)
2016-09-20 01:40:22     166.123.218.220 17456    udp@attack@amp_flood_target-NTP irs.gov->A:166.123.218.220(domain_chain)
2016-09-20 01:46:08     166.123.218.220 4444     udp@attack@amp_flood_target-DNS irs.gov->A:166.123.218.220(domain_chain)
2016-09-20 01:35:29     166.123.218.220 27272    udp@attack@amp_flood_target-NTP irs.gov->A:166.123.218.220(domain_chain)
2016-09-20 01:35:17     166.123.218.220 62565    udp@attack@amp_flood_target-NTP irs.gov->A:166.123.218.220(domain_chain)
2016-09-20 01:35:15     166.123.218.220 6202     udp@attack@amp_flood_target-NTP irs.gov->A:166.123.218.220(domain_chain)
2016-09-20 01:36:44     166.123.218.220 0        udp@attack@amp_flood_target-FRGM        irs.gov->A:166.123.218.220(domain_chain)
2016-09-20 01:36:36     166.123.218.220 4444     udp@attack@amp_flood_target-DNS irs.gov->A:166.123.218.220(domain_chain)
2016-09-20 01:35:16     166.123.218.220 38836    udp@attack@amp_flood_target-NTP irs.gov->A:166.123.218.220(domain_chain)
2016-09-20 01:35:57     166.123.218.220 38836    udp@attack@amp_flood_target-NTP irs.gov->A:166.123.218.220(domain_chain)
2016-09-20 01:36:23     166.123.218.220 62980    udp@attack@amp_flood_target-NTP irs.gov->A:166.123.218.220(domain_chain)
2016-09-20 01:58:38     152.216.011.133 0        udp@attack@amp_flood_target-FRGM        ns4.irs.gov->A:152.216.011.133(domain_chain)
2016-09-20 01:57:58     152.216.007.164 4444     udp@attack@amp_flood_target-DNS ns1.irs.gov->A:152.216.007.164(domain_chain)
2016-09-20 01:40:22     166.123.218.220 55210    udp@attack@amp_flood_target-NTP irs.gov->A:166.123.218.220(domain_chain)
2016-09-20 02:09:50     152.216.007.165 4444     udp@attack@amp_flood_target-DNS ns2.irs.gov->A:152.216.007.165(domain_chain)
2016-09-20 01:58:38     152.216.011.133 4444     udp@attack@amp_flood_target-DNS ns4.irs.gov->A:152.216.011.133(domain_chain)
2016-09-20 01:58:16     152.216.011.132 0        udp@attack@amp_flood_target-FRGM        ns3.irs.gov->A:152.216.011.132(domain_chain)
```

More Details See: https://ddosmon.net/explore/irs.gov/

Case: irs.gov

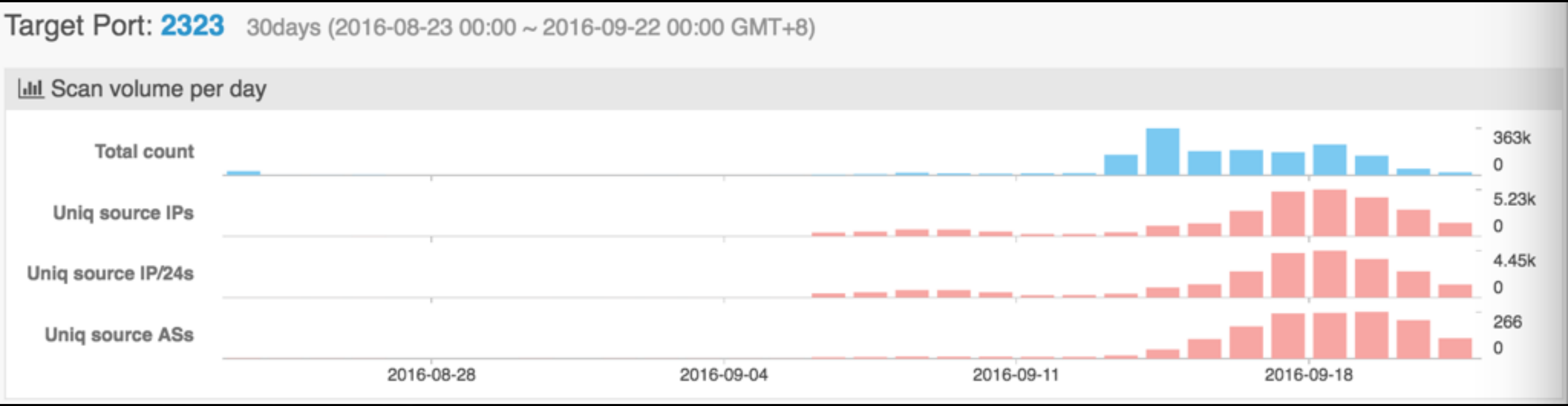


```
[xuamao@xuamaos-MacBook-Pro:~]$ sdanf 166.123.218.220 --last 240 -l 15 | sort
2016-09-20 01:24:20     166.123.218.220 0       udp@attack@amp_flood_target-FRGM;DNS
2016-09-20 01:25:08     166.123.218.220 4444    dns@attack@fake_query_client     cpsc.gov=12(fqdn_str)
2016-09-20 01:35:08     166.123.218.220 4444    dns@attack@amp_flood_target      cpsc.gov=74(fqdn_str)
2016-09-20 01:35:15     166.123.218.220 6202    udp@attack@amp_flood_target-NTP
2016-09-20 01:35:16     166.123.218.220 38836   udp@attack@amp_flood_target-NTP
2016-09-20 01:35:17     166.123.218.220 62565   udp@attack@amp_flood_target-NTP
2016-09-20 01:35:29     166.123.218.220 27272   udp@attack@amp_flood_target-NTP
2016-09-20 01:35:57     166.123.218.220 38836   udp@attack@amp_flood_target-NTP
2016-09-20 01:36:05     166.123.218.220 17511   udp@attack@amp_flood_target-NTP
2016-09-20 01:36:23     166.123.218.220 62980   udp@attack@amp_flood_target-NTP
2016-09-20 01:36:36     166.123.218.220 4444    udp@attack@amp_flood_target-DNS
2016-09-20 01:36:44     166.123.218.220 0       udp@attack@amp_flood_target-FRGM
2016-09-20 01:40:08     166.123.218.220 4444    dns@attack@amp_flood_target      cpsc.gov=294(fqdn_str)
2016-09-20 01:40:21     166.123.218.220 0       udp@attack@amp_flood_target-NTP;DNS
2016-09-20 01:40:22     166.123.218.220 17456   udp@attack@amp_flood_target-NTP
2016-09-20 01:45:08     166.123.218.220 4444    dns@attack@amp_flood_target      cpsc.gov=462(fqdn_str)
2016-09-20 01:46:05     166.123.218.220 0       udp@attack@amp_flood_target-FRGM
2016-09-20 01:46:08     166.123.218.220 4444    udp@attack@amp_flood_target-DNS
2016-09-20 01:46:08     166.123.218.220 4444    udp@attack@amp_flood_target-DNS
2016-09-20 01:50:08     166.123.218.220 4444    dns@attack@amp_flood_target      cpsc.gov=311(fqdn_str)
2016-09-20 01:55:11     166.123.218.220 4444    dns@attack@amp_flood_target      cpsc.gov=138(fqdn_str)
2016-09-20 02:00:08     166.123.218.220 4444    dns@attack@amp_flood_target      cpsc.gov=78(fqdn_str)
```

More Details See: https://ddosmon.net/explore/166.123.218.220/

Case: Mirai Trojan

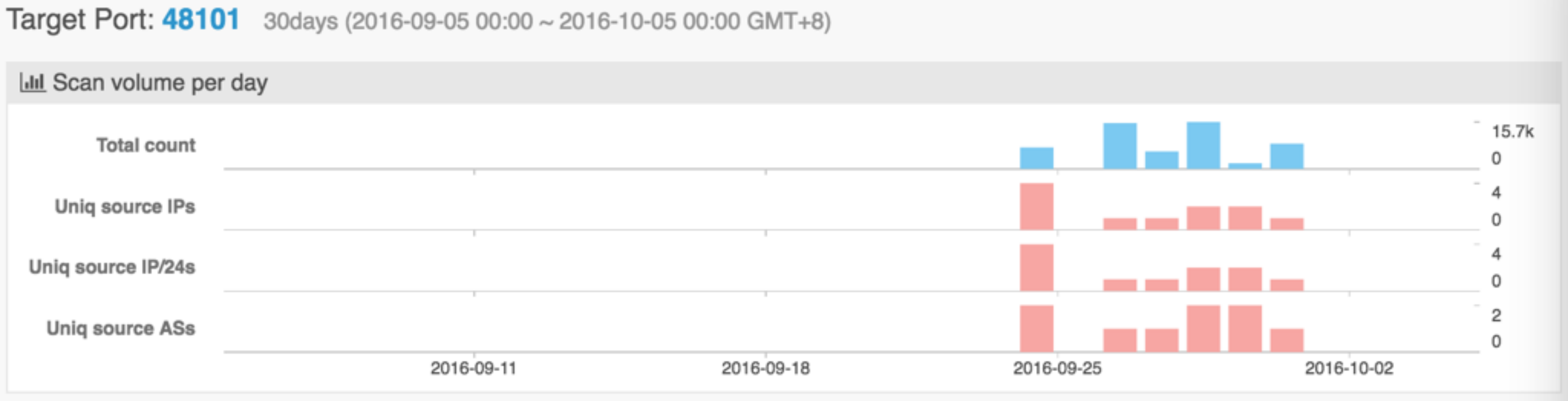
http://news.softpedia.com/news/mirai-ddos-trojan-is-the-next-big-threat-for-iot-devices-and-linux-servers-507964.shtml



Target Port: 2323 30days (2016-08-23 00:00 ~ 2016-09-22 00:00 GMT+8)

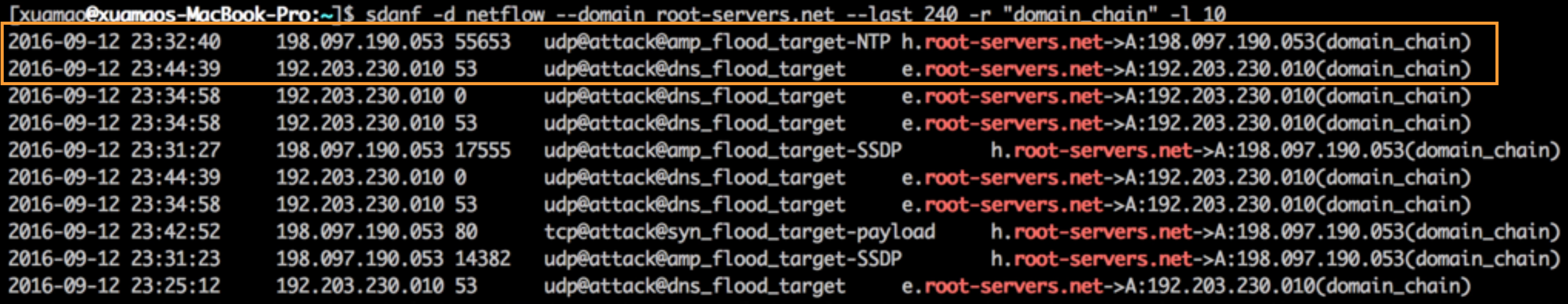
Case: Mirai Trojan

https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html



Target Port: **48101** 30days (2016-09-05 00:00 ~ 2016-10-05 00:00 GMT+8)

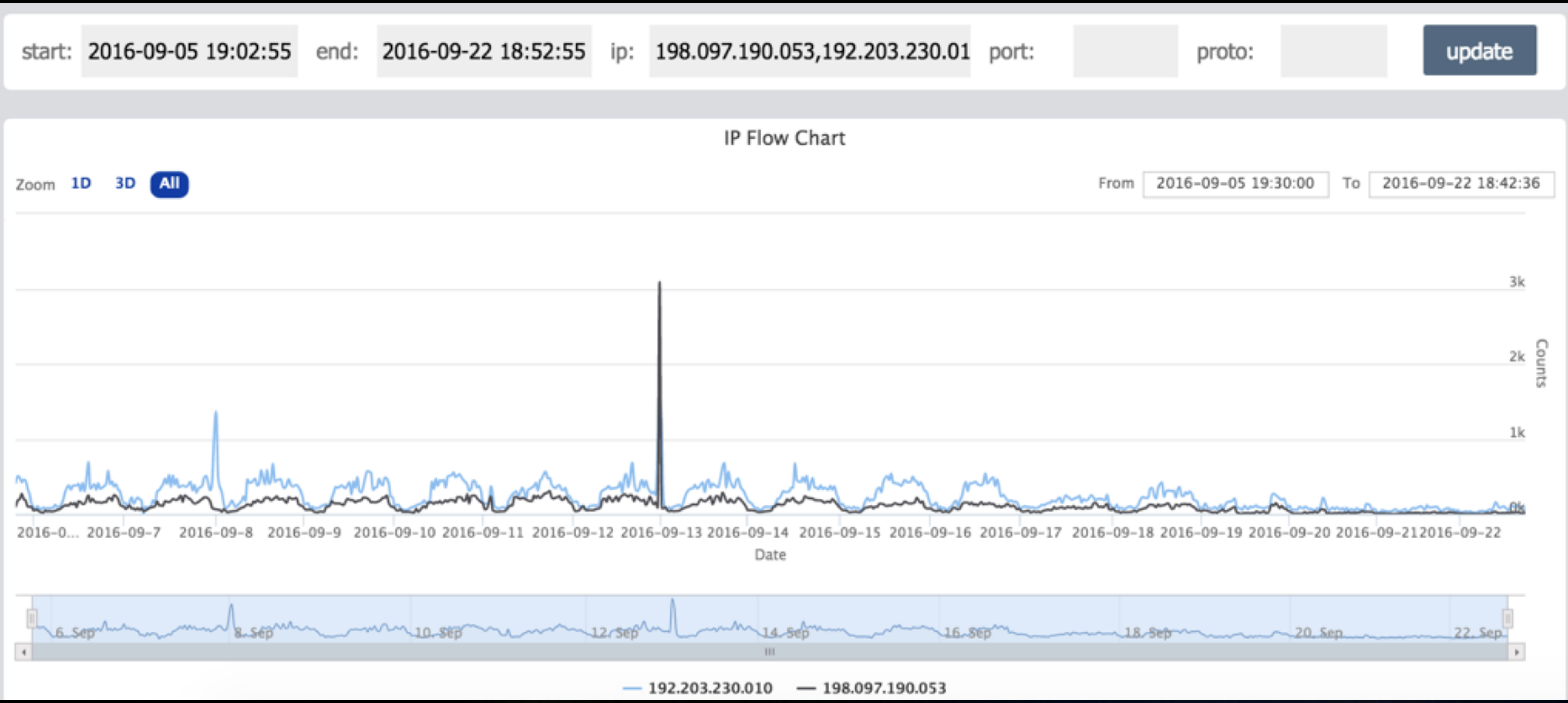
Case: *.root-servers.net



```
[xuamao@xuamaos-MacBook-Pro:~]$ sdanf -d netflow --domain root-servers.net --last 240 -r "domain_chain" -l 10
2016-09-12 23:32:40     198.097.190.053 55653   udp@attack@amp_flood_target-NTP h.root-servers.net->A:198.097.190.053(domain_chain)
2016-09-12 23:44:39     192.203.230.010 53      udp@attack@dns_flood_target     e.root-servers.net->A:192.203.230.010(domain_chain)
2016-09-12 23:34:58     192.203.230.010 0       udp@attack@dns_flood_target     e.root-servers.net->A:192.203.230.010(domain_chain)
2016-09-12 23:34:58     192.203.230.010 53      udp@attack@dns_flood_target     e.root-servers.net->A:192.203.230.010(domain_chain)
2016-09-12 23:31:27     198.097.190.053 17555   udp@attack@amp_flood_target-SSDP        h.root-servers.net->A:198.097.190.053(domain_chain)
2016-09-12 23:44:39     192.203.230.010 0       udp@attack@dns_flood_target     e.root-servers.net->A:192.203.230.010(domain_chain)
2016-09-12 23:34:58     192.203.230.010 53      udp@attack@dns_flood_target     e.root-servers.net->A:192.203.230.010(domain_chain)
2016-09-12 23:42:52     198.097.190.053 80      tcp@attack@syn_flood_target-payload     h.root-servers.net->A:198.097.190.053(domain_chain)
2016-09-12 23:31:23     198.097.190.053 14382   udp@attack@amp_flood_target-SSDP        h.root-servers.net->A:198.097.190.053(domain_chain)
2016-09-12 23:25:12     192.203.230.010 53      udp@attack@dns_flood_target     e.root-servers.net->A:192.203.230.010(domain_chain)
```

More Details See: https://ddosmon.net/explore/root-servers.net/

Case: *.root-servers.net

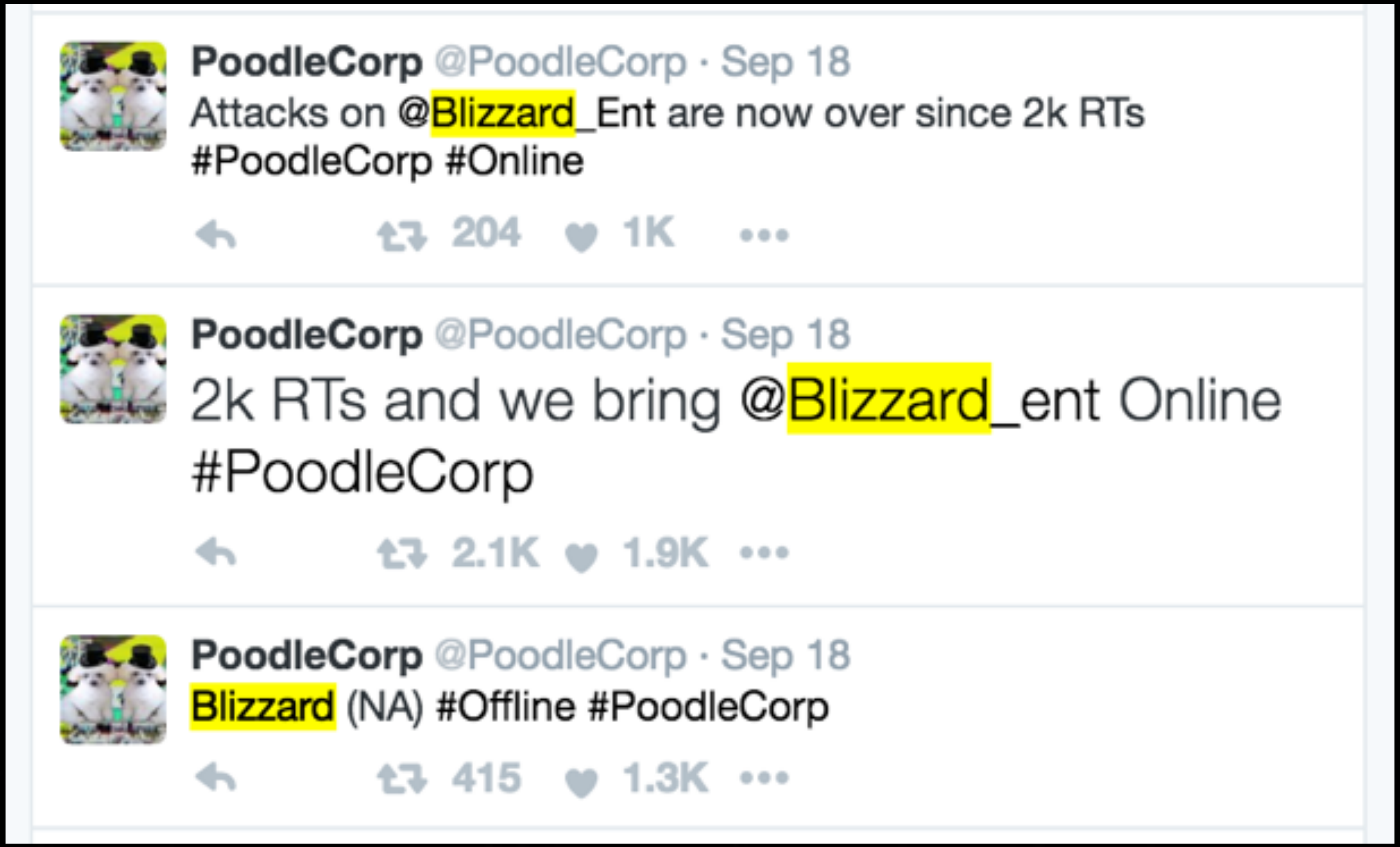


start: 2016-09-05 19:02:55 end: 2016-09-22 18:52:55 ip: 198.097.190.053,192.203.230.01 port: proto:

IP Flow Chart

From 2016-09-05 19:30:00 To 2016-09-22 18:42:36

Case: *.battle.net



PoodleCorp @PoodleCorp · Sep 18
Attacks on @Blizzard_Ent are now over since 2k RTs #PoodleCorp #Online
204 1K

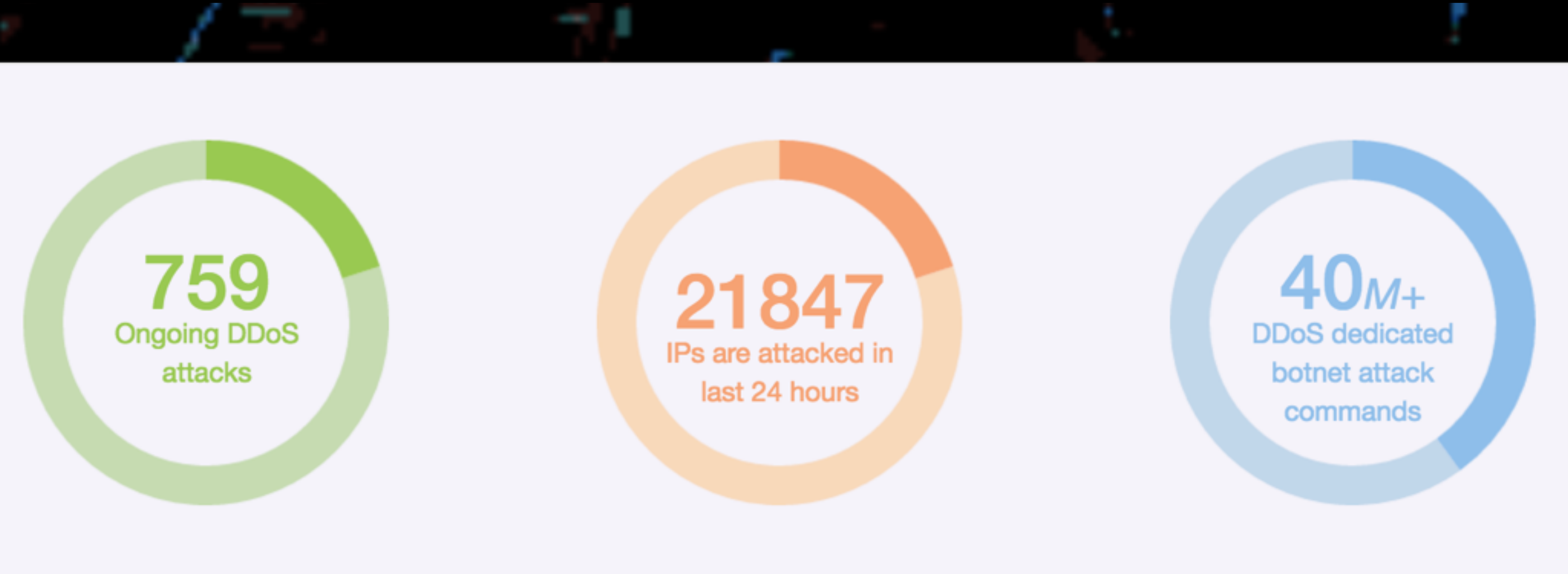
PoodleCorp @PoodleCorp · Sep 18
2k RTs and we bring @Blizzard_ent Online #PoodleCorp
2.1K 1.9K

PoodleCorp @PoodleCorp · Sep 18
Blizzard (NA) #Offline #PoodleCorp
415 1.3K

```
[xuyang-pd@dev1:~]$ sdanf -d netflow --domain battle.net -t attack --last 240 -r domain_chain
2016-09-22 08:38:37     024.105.029.040 0       udp@attack@amp_flood_target-NTP                 us.battle.net->A:024.105.029.040(domain_chain)
2016-09-19 10:44:13     024.105.029.040 0       udp@attack@amp_flood_target-FRGM;DNS            us.battle.net->A:024.105.029.040(domain_chain)
```

More Details See: https://ddosmon.net/explore/battle.net/

https://ddosmon.net/

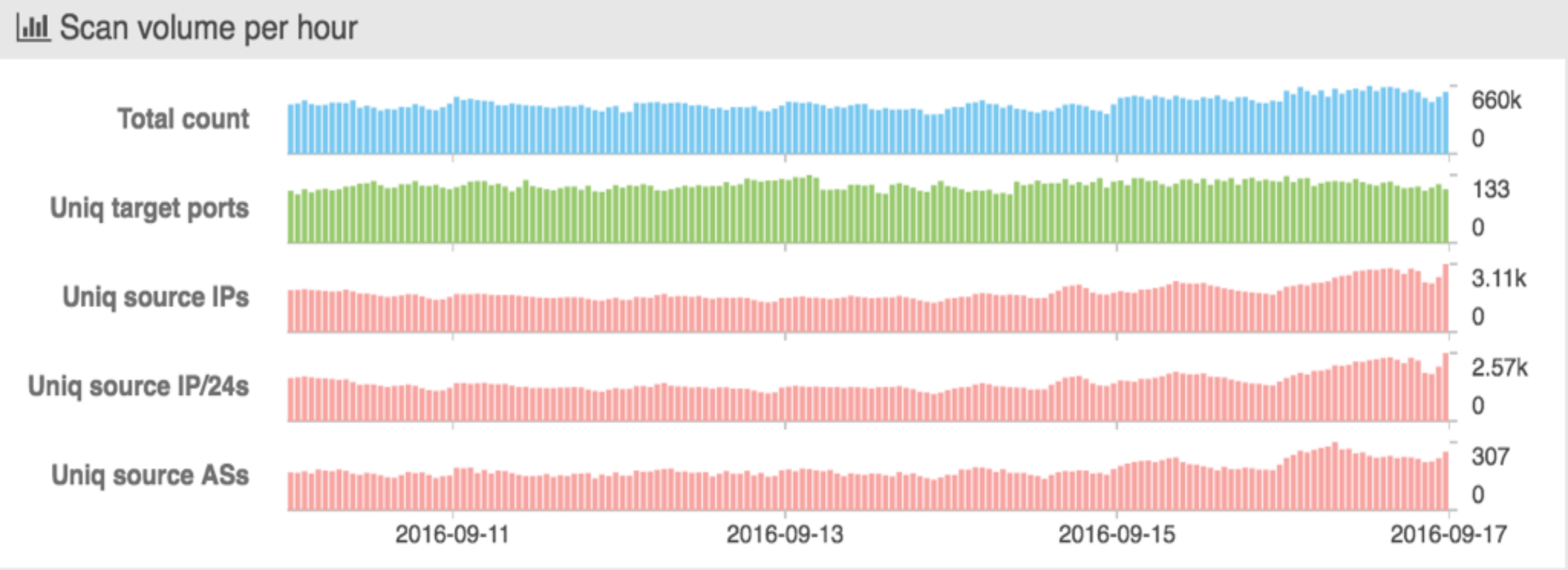


759
Ongoing DDoS attacks

21847
IPs are attacked in last 24 hours

40M+
DDoS dedicated botnet attack commands

http://scan.netlab.360.com/



Thanks

```
.dsetsize <= NGROUPS_SM.
group_info->blocks[0] = grou,
else {
for (                 e; i++) {
                      _free_page
                o out_undo_par
              _info->bloc
ial_alloc:
i >= 0) {
```