

# Backbone Network DRDoS Attack Monitoring and Analysis

YANG XU, QITIAN SU

Twitter: @xuy1202 @suqitian

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 DRDoS

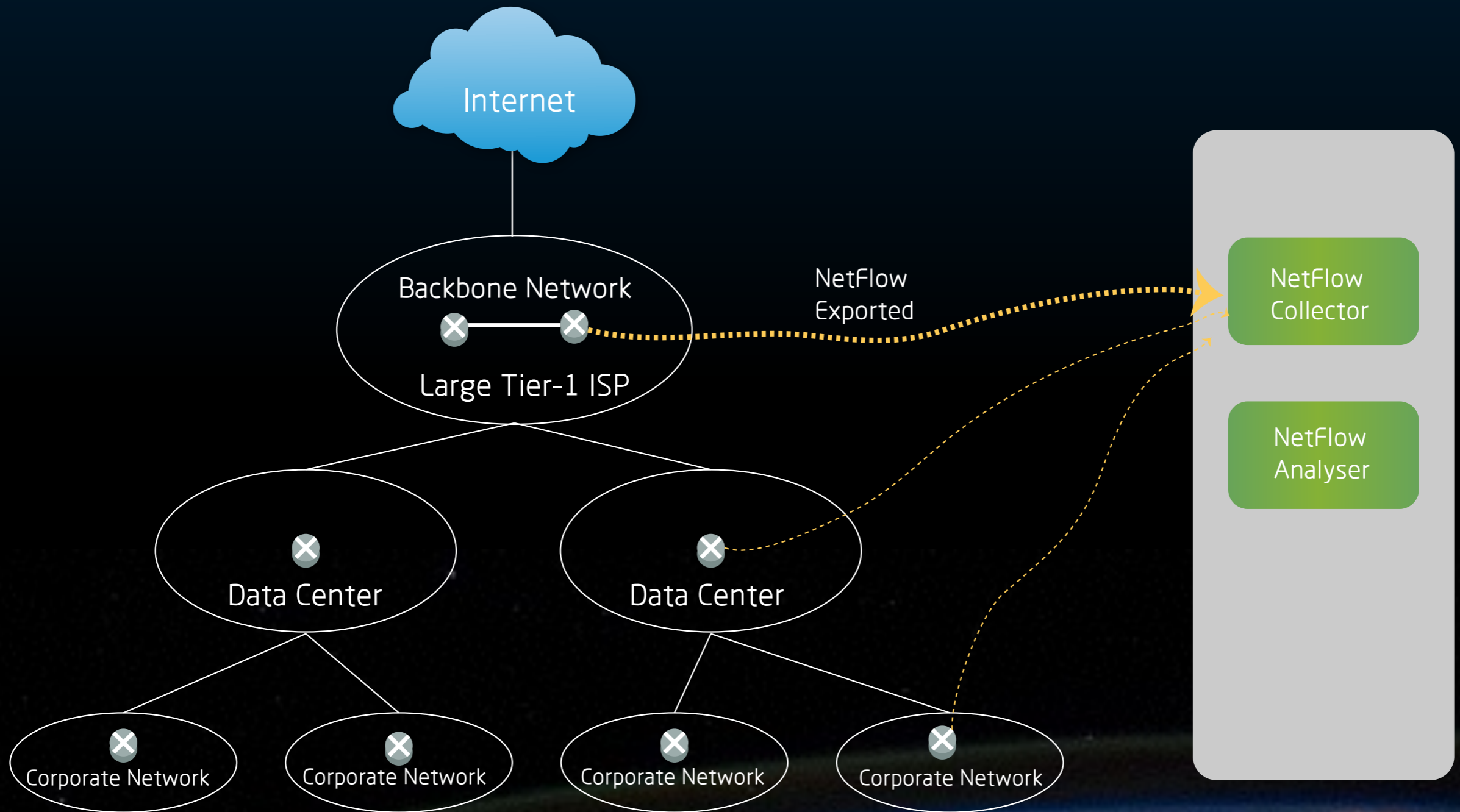
Most Popular DDoS Method

Un-control Side Effects

Hard To Trace

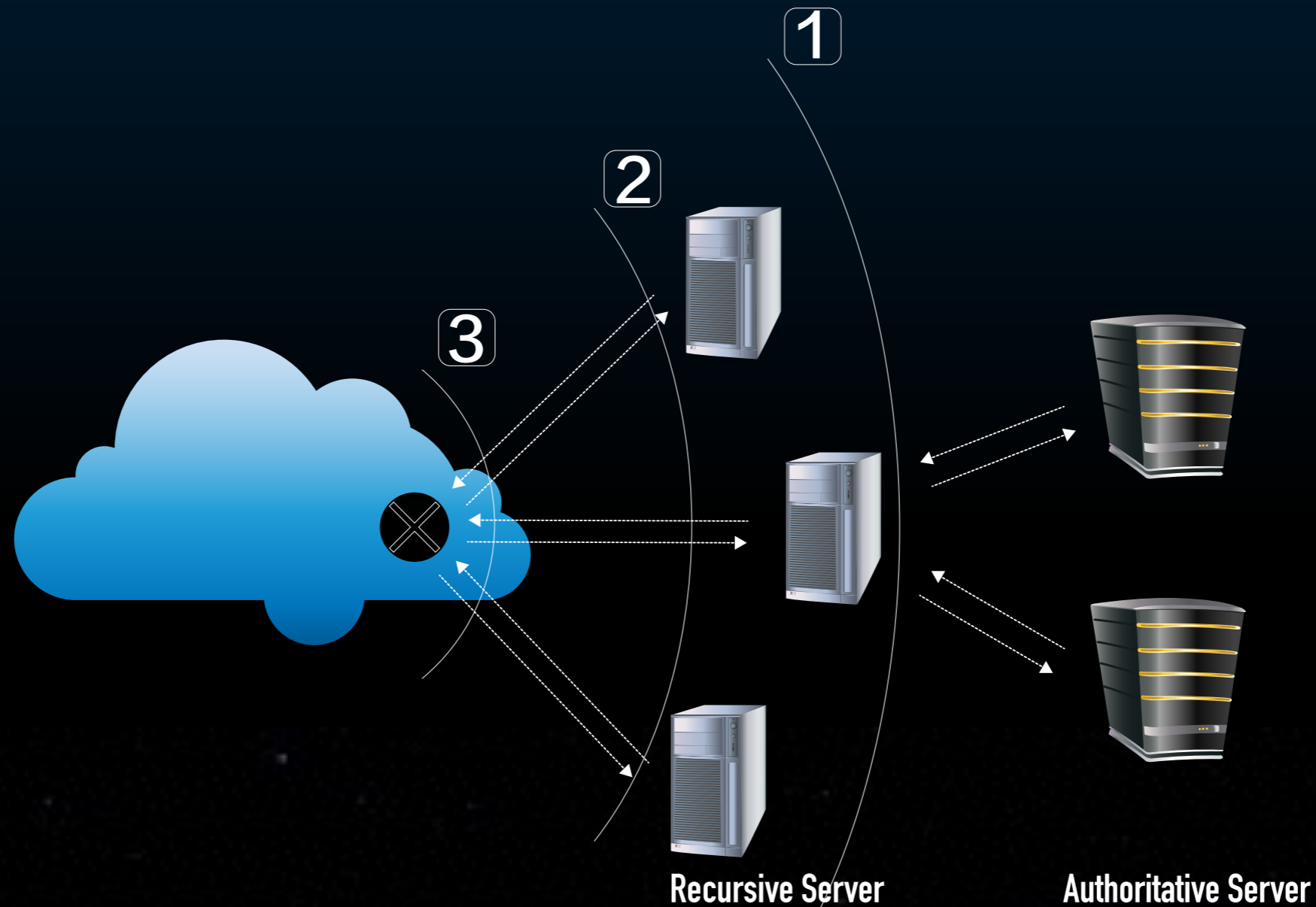
Lasting Damage

# NetFlow Collecting





# PDNS Collecting



1: small data; clean data

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

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

3: client focused perspective, richer info

# BIIG Data

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

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

200 M IP' s Activities / per day


1/10 of Chinese DNS data, 99% coverage of Chinese Domain

IPv6 only accounts less than 5% of all traffic in China, now we don't take it into consideration.

# Case in Netflow


## Attack Time Line

Detected **5** 35.161.1.80 related events in last 24 hours and **5** events in last 30 days.

IP: 35.161.1.80  
Protocol: UDP  
Port: ALL  
Types: udp@attack@amp\_flood\_target-DNS,  
udp@attack@amp\_flood\_target  
Traffic: 

2016-12-09  
16:07:48

2016-12-09  
14:59:20

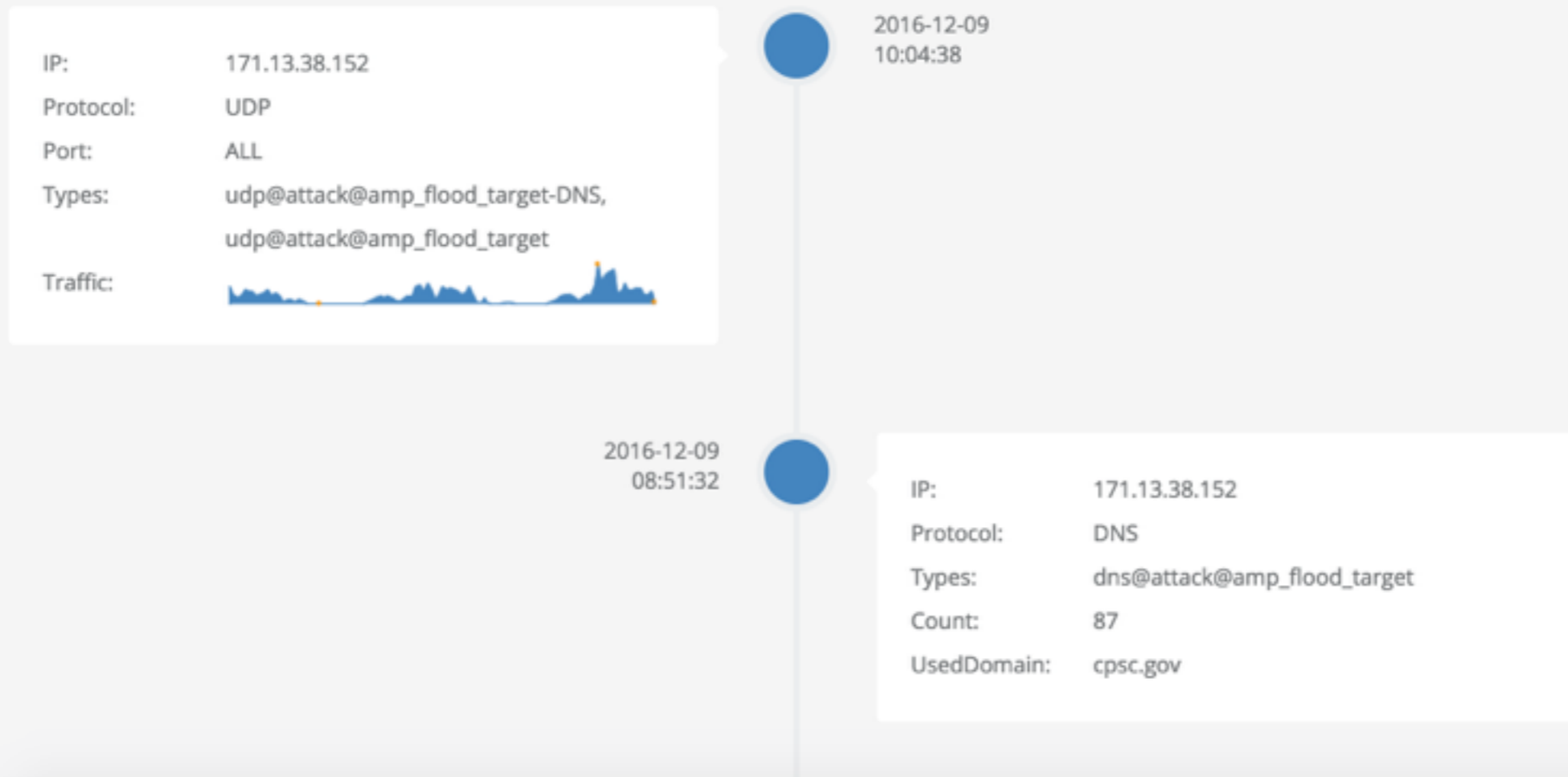
IP: 35.161.1.80  
Protocol: UDP  
Port: ALL  
Types: udp@attack@amp\_flood\_target-DNS,  
udp@attack@amp\_flood\_target,  
udp@attack@simple\_flood\_target  
Traffic: 

<https://ddosmon.net/explore/35.161.1.80>

# Case in DNS

## Attack Time Line

Detected **6** 171.13.38.152 related events in last 24 hours and **31** events in last 30 days.



<https://ddosmon.net/explore/171.13.38.152>



# Attack Fail Case

ICMP Unreachable (0x0300 - 0x030f)

cpsec.gor\013

# Attack Events Statistic

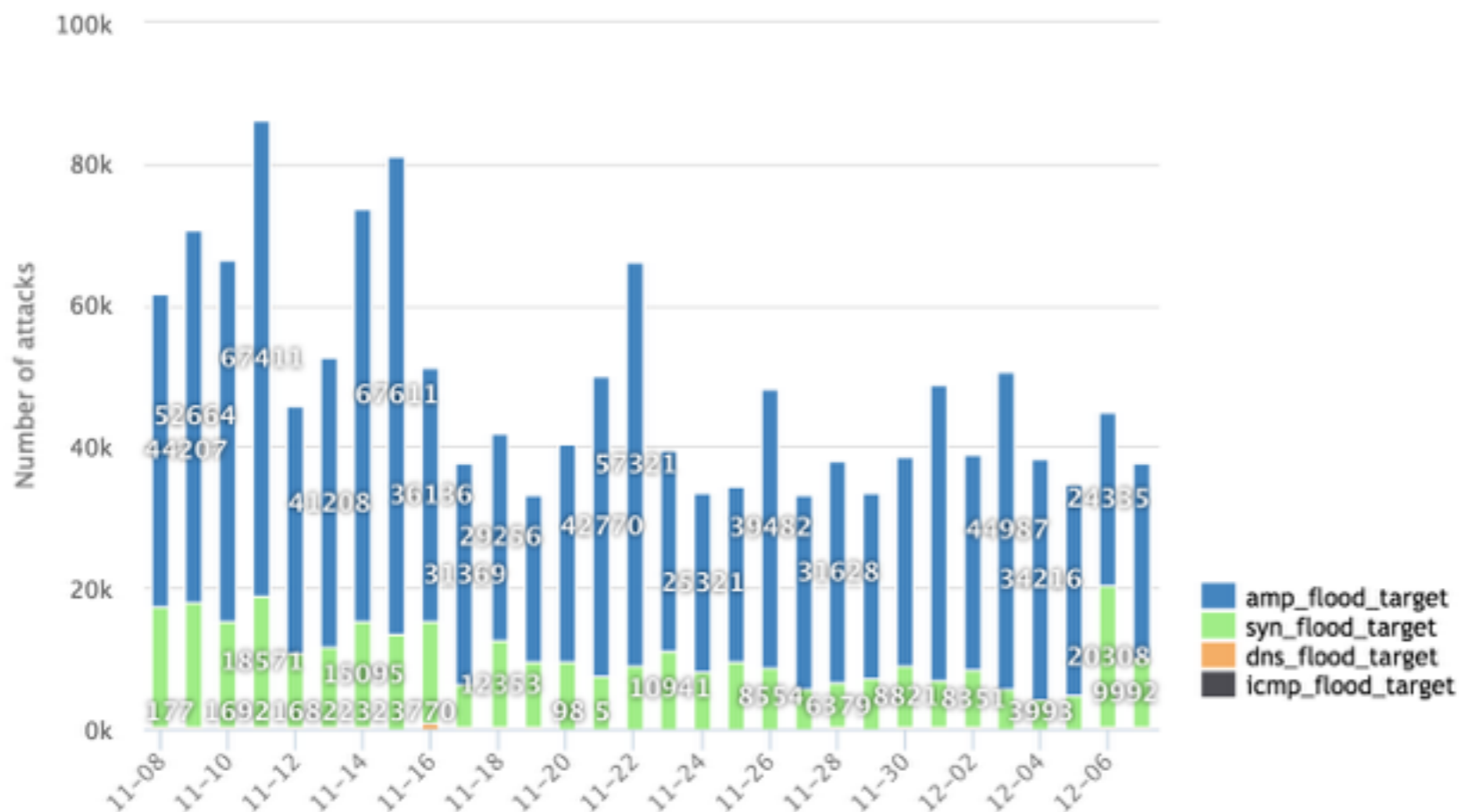
Daily Average DDoS Events 37w+, for 5w+ victim IPs

Daily Average DRDoS Events 25w+, for 3w+ victim IPs

DRDoS accounted for 65%+ of all DDoS attacks

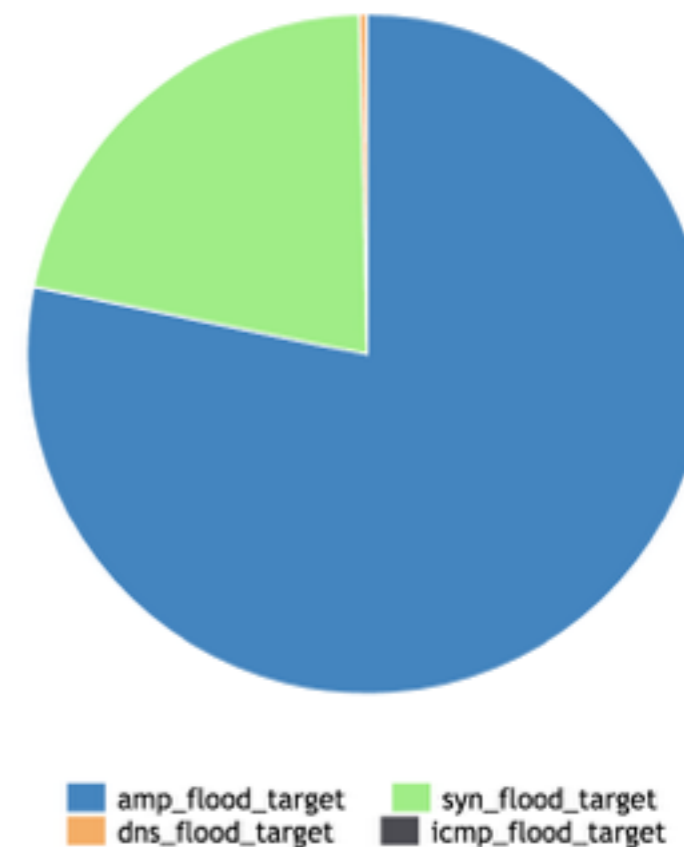
Attack trending

In last 30 days

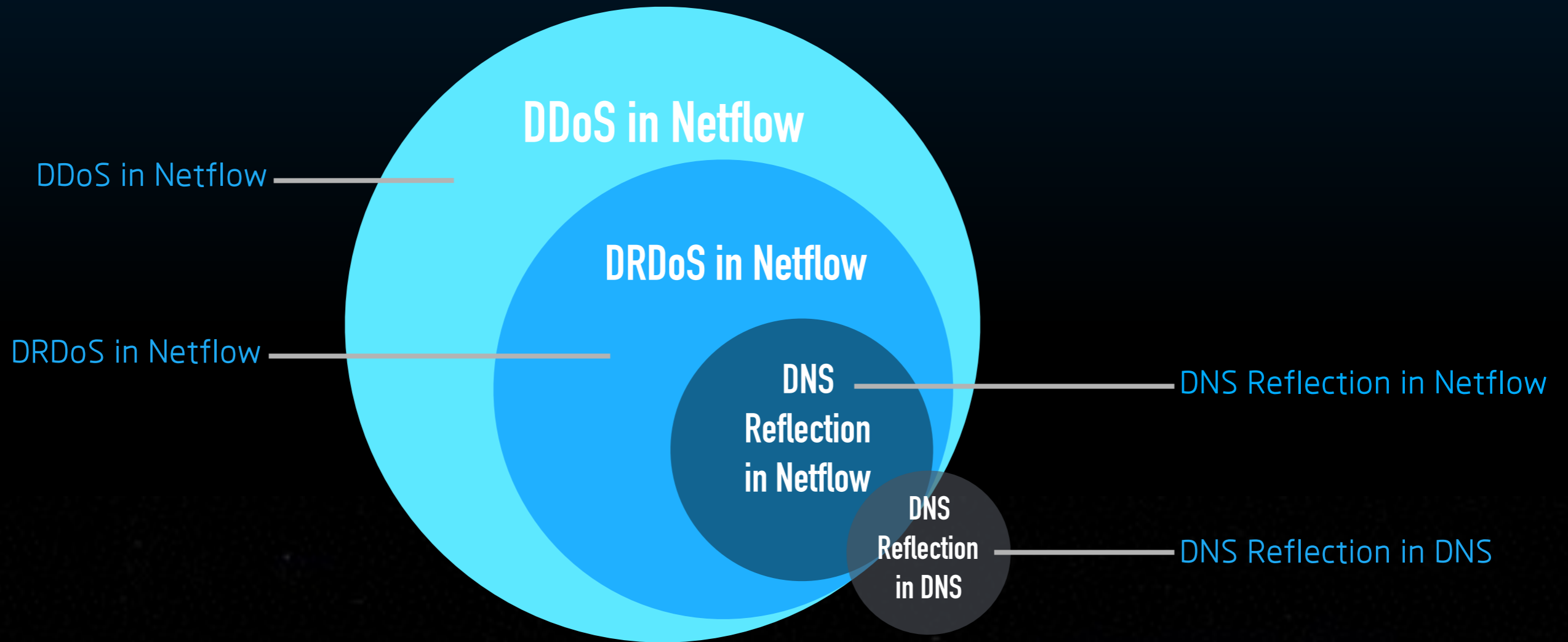


Attack vectors statistics

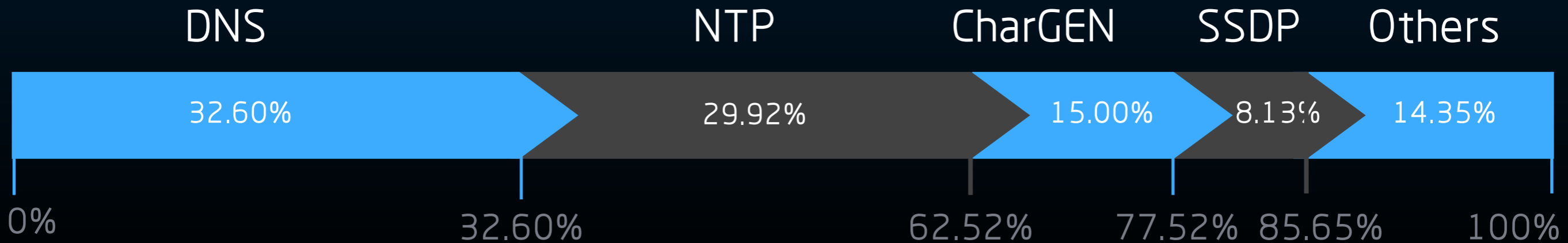
In last 30 days



# Cross Validation



# DRDoS Attack Vector



## DETAILS

32.60%	32.60%	DNS
62.52%	29.92%	NTP
77.52%	15.00%	CharGEN
85.65%	8.13%	SSDP
87.69%	2.04%	NTP + DNS
89.65%	1.96%	BitTorrent
91.18%	1.53%	L2TP
92.17%	0.99%	NTP + SSDP
93.14%	0.97%	NTP + SNMP
93.99%	0.85%	NTP + TFTP + SNMP
94.74%	0.75%	L2TP + DNS
95.40%	0.66%	SNMP
95.94%	0.54%	NTP + SNMP
96.48%	0.54%	SSDP + CharGEN
97.01%	0.53%	LDAP
100.0%	2.99%	Others

Big Head / Stable Proportion

Detection of New Vector, like TFTP / LDAP



# DNS Reflection Attack Vector



## DETAILS

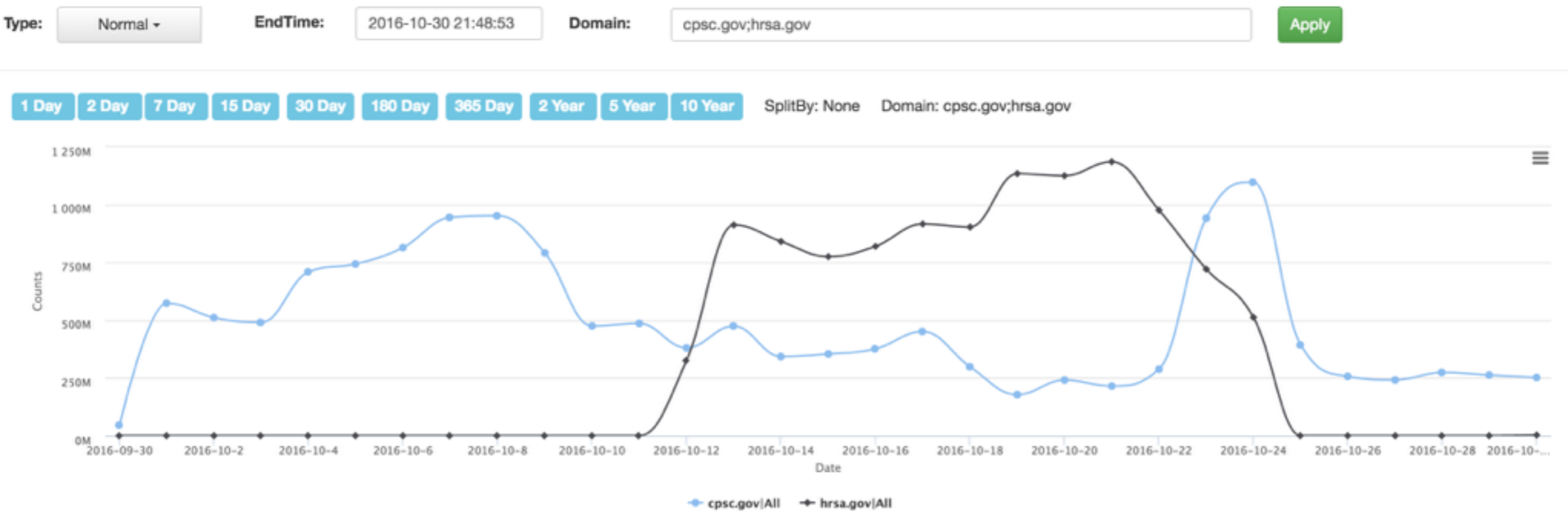
65.25%	65.25%	cpssc.gov
80.22%	17.97%	defcon.org
84.98%	4.76%	aids.gov
88.96%	3.98%	1x1.cz
91.38%	2.42%	kth.se
93.21%	1.83%	nih.gov
94.42%	1.21%	commerce.gov
95.01%	0.59%	isc.org
95.43%	0.42%	wapa.gov
95.77%	0.34%	hoffmeister.be
96.07%	0.30%	doc.gov
96.34%	0.27%	activum.nu
96.58%	0.24%	leth.cc
96.81%	0.23%	d51.ru
96.97%	0.16%	defcongroups.org
100.0%	3.03%	Others

Big Big Head

Some new domain will appear from time to time: hrsa.gov



# DNS Reflection Attack Vector



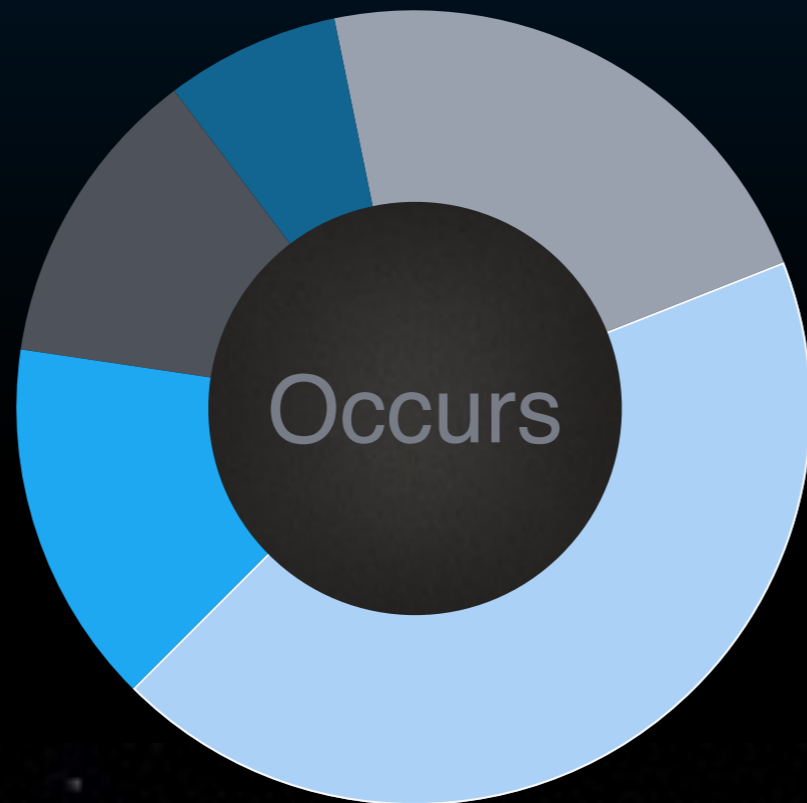
# Block Domain Query?

Change DNS Records?

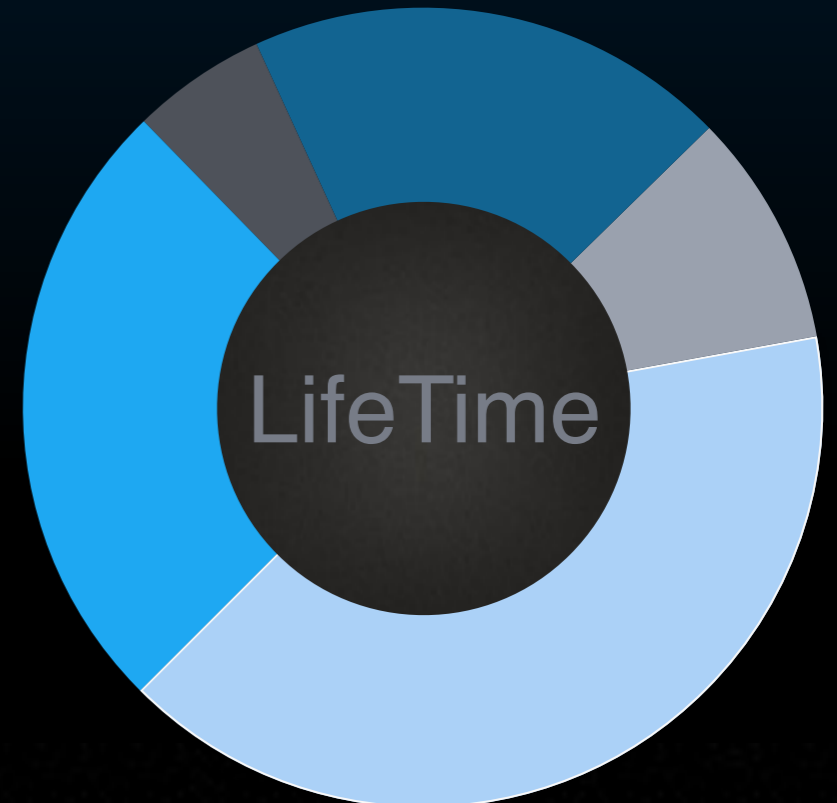
Normal Query vs. Spoofed Attack Query?

Block "ANY Query" ?

# ALL Amplifier In Netflow



- count == 1
- count == 2
- count == 3
- 3 < count < 10
- count >= 10



- time == 0
- 0 < time <= 1 hour
- 1 hour < time <= 12 hours
- 12 hours < time <= 24 hours
- time > 1 day

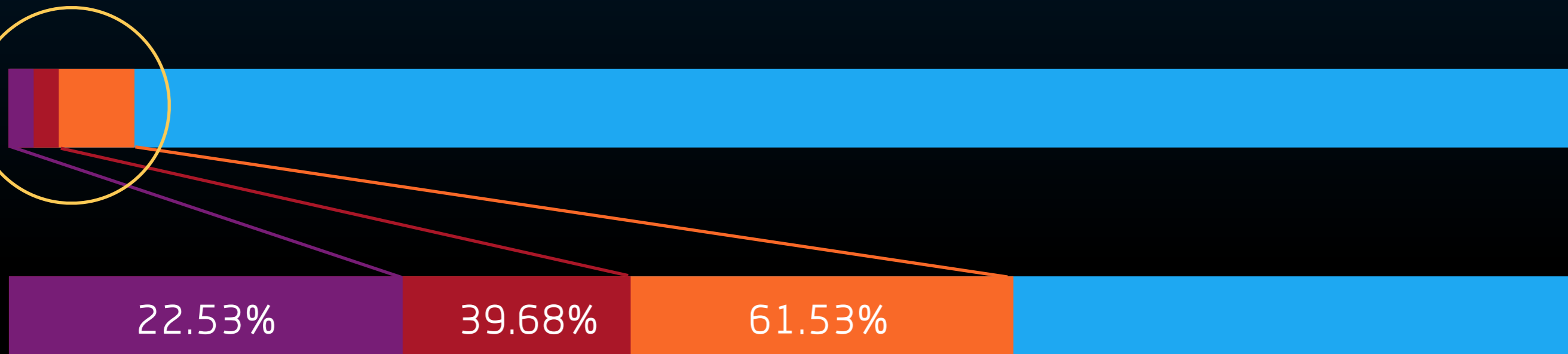


DETAILS

Events	Unique IPs	Service
97265531	4111887	ALL
89749356	3928766	SSDP
4860920	58404	NTP
1345522	85237	DNS
517370	9970	Portmap
679896	8330	CharGEN
52162	8858	SNMP
22206	10013	Kad
19067	505	TFTP
12588	4100	mDNS
6444	1804	Others

# DNS Amplifier In Netflow

In Last 6 Months: 1345522 DNS Amplifier Events , 85237 Unique Amplifier IPs

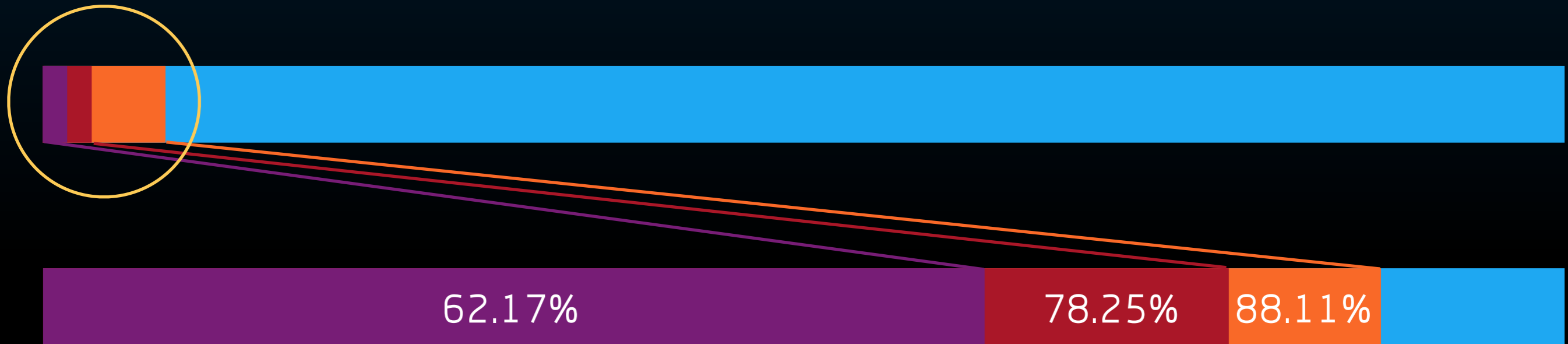


	Unique IPs	Attack Events	
<b>TOP1000</b>	1.2%	303088	22.53%
<b>TOP3000</b>	3.5%	533893	39.68%
<b>TOP9000</b>	10.5%	827821	61.53%



# DNS Amplifier In DNS

In Last 30 days: 143491 DNS Amplifier Events , 6175 Unique Amplifier IPs

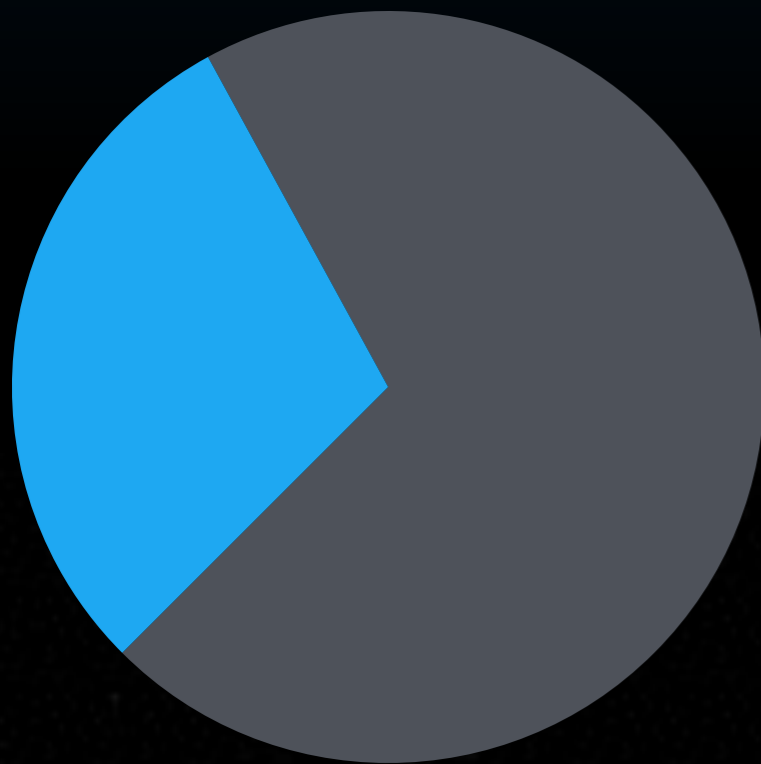


	Unique IPs	Attack Events
<b>TOP100</b>	1.6%	89205 62.17%
<b>TOP200</b>	3.2%	112283 78.25%
<b>TOP500</b>	8.1%	126434 88.11%



# DNS Amplifier

All DNS Amplifier  
validated in PDNS data



- Authority Server
- UnKnown

All Unknown  
dig scan



- Live Open Resolver
- Dead
- Unknown Authority Server

Live Open Resolver  
statistic of 30 days data



- Attack Queries Only
- Combined Queries

# Block Amplifier?

Near Source vs. Near Target?

Block or "Partial Block" ?

Self Block?

# Further Work

<https://ddosmon.net/> // realtime DDoS attcks

<http://data.netlab.360.com/> // all kinds of open data

Share ideas, share data, hands together, for better cyber.

# Thanks

```
...dsetsize <= NGROUPS_8B...  
group_info->blocks[0] = grou...  
else {  
  for (i = 0; i < n; i++) {  
    ...free_page
```

```
...out_undo_part...  
..._info->block
```

```
...ial_alloc...  
...i >= 0) {  
  ...
```