Backbone Network DRDoS Attack Monitoring and Analysis

YANG XU

Twitter: @xuy1202

Network Security Research Lab, Qihoo 360

http://netlab.360.com/

Our Team, Our Goal

Threat Research, Security Basic Data, See More:

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

What We Have Done

Daily Average

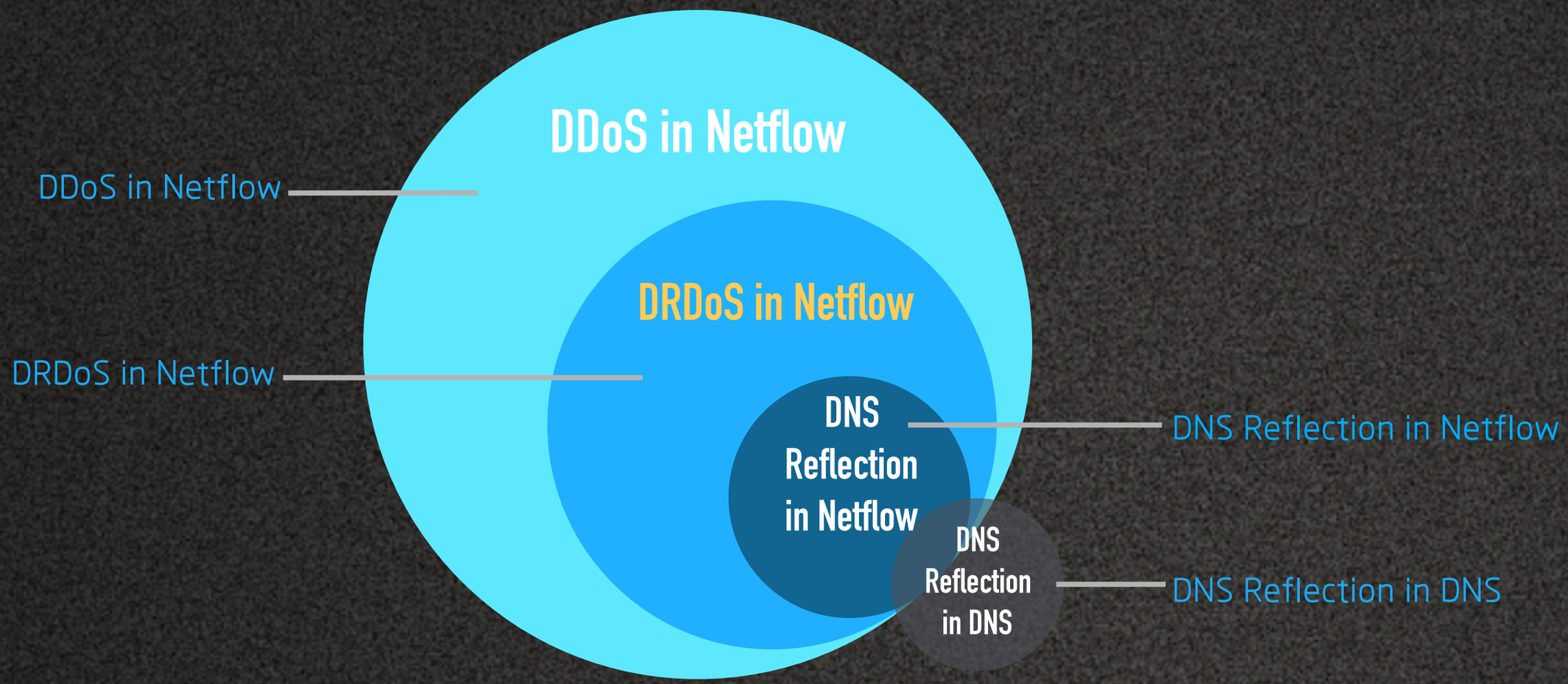
350K+ DDoS Events to 50K+ victim IPs

500K+ Bot-net attacking instructions to 3K+ victim IPs
from 200+ CNC activities of 30+ Bot-net Families

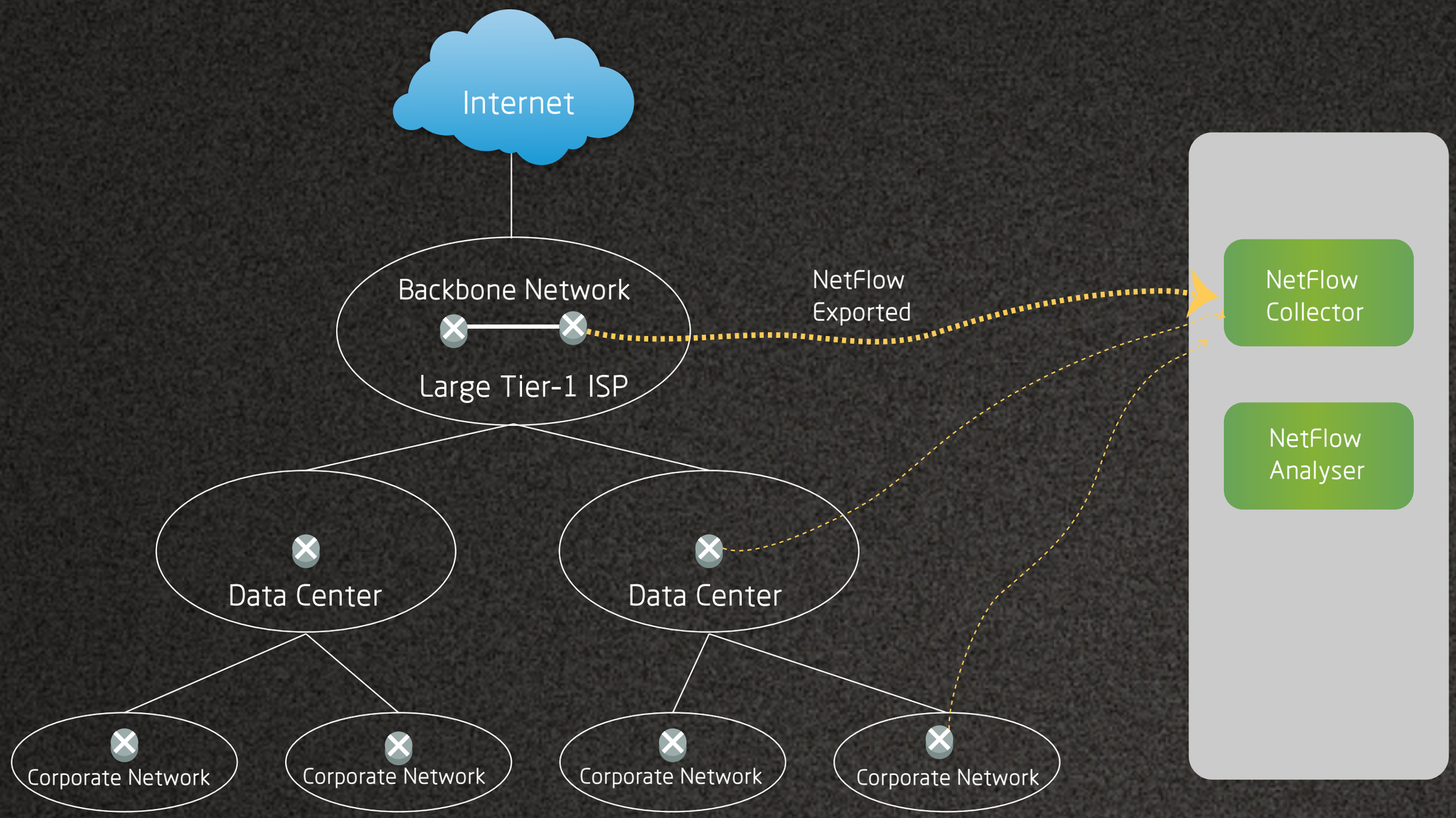
Why DRDoS

Daily Average DRDoS Events 250k+, for 30k+ victim IPs, DRDoS accounted for 60%+ of all DDoS attacks

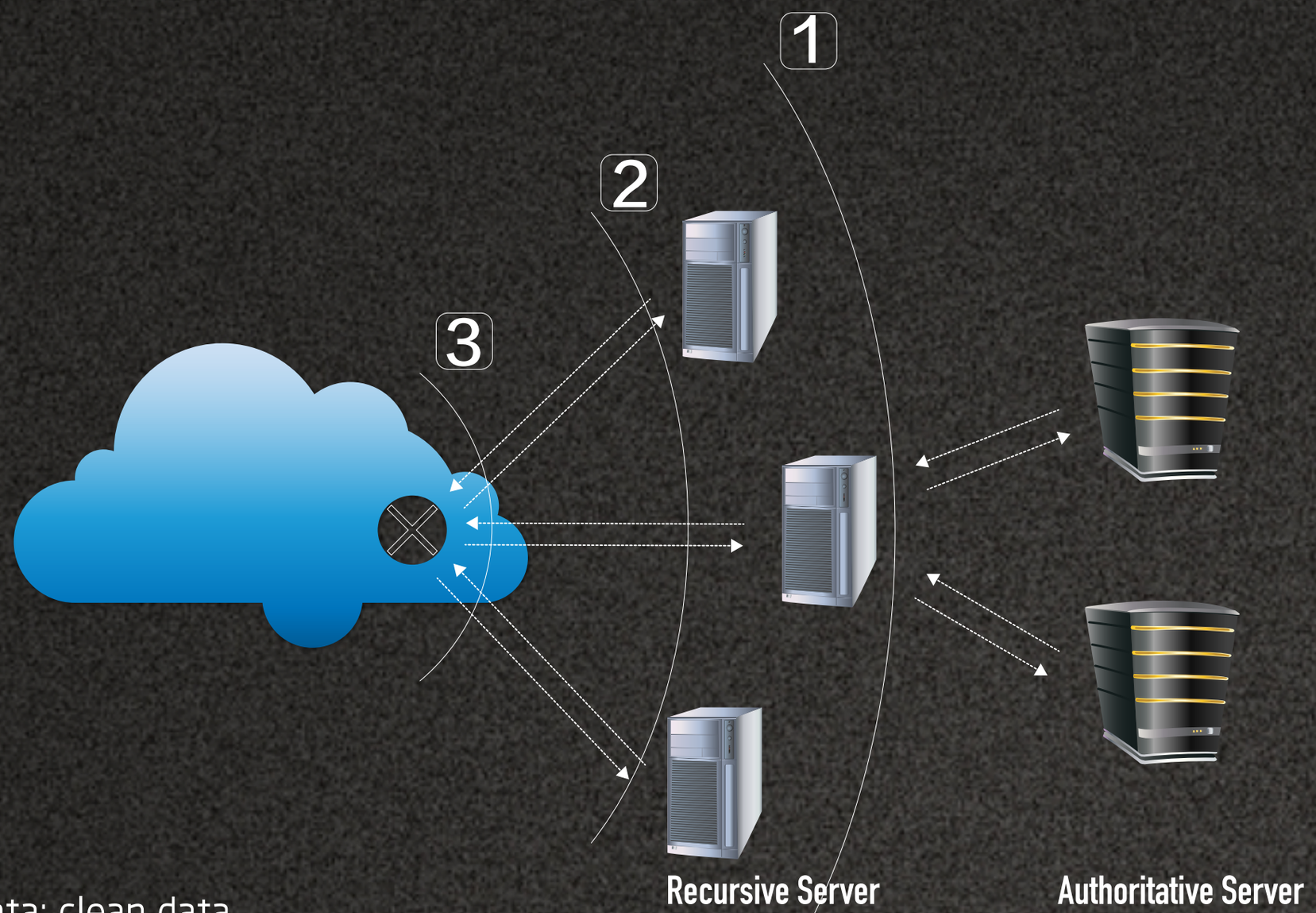
1. Most popular DDoS method
2. Hard to trace
3. Un-control side effects
4. Take it rather than defeat it



NetFlow Collecting



PDNS Collecting



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

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

BIIIG Data

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

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

Backbone router original traffic volume up to 9T+ bps

200 M+ IP’s Activities / per day [1]

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

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

Detection Model

rule-based, realtime statistic in adaptive time window

- 3 Levels: IP / IP-Proto / IP-Proto-Port
- 2 Directions: IN / OUT
- 50+ Features:

  Distribution / Top / Continuity / Unique Count / Average …

  of

  Flow / IP / Port / Flow Duration / Packages / Package Size …

Case in NetFlow

DDOS MON

STATISTIC APPLY SIGN IN

Attack Time Line

Detected 0 krebsonsecurity.com related events in last 24 hours and 2 events in last 30 days.

2017-01-07
02:54:03

IP:	130.211.45.45
Protocol:	TCP
Port:	ALL
Types:	tcp@attack@syn_flood_target-mix_RST
Chains:	krebsonsecurity.com => 130.211.45.45 www.krebsonsecurity.com => 130.211.45.45
Traffic:	

2016-12-19
17:04:02

IP:	130.211.45.45
Protocol:	UDP,TCP
Port:	ALL
Types:	tcp@attack@syn_flood_target, udp@attack@simple_flood_target, tcp@attack@syn_flood_target-payload
Chains:	krebsonsecurity.com => 130.211.45.45

https://ddosmon.net/explore/krebsonsecurity.com

Case in NetFlow

DDOS MON

STATISTIC APPLY SIGN IN

Attack Time Line

Detected 0 donaldjtrump.com related events in last 24 hours and 1 events in last 30 days.

IP:	104.16.75.120
Protocol:	UDP
Port:	ALL
Types:	udp@attack@amp_flood_target-DNS, udp@attack@amp_flood_target
Chains:	assets.donaldjtrump.com => 104.16.75.120
	donaldjtrump.com => 104.16.75.120
	secure.donaldjtrump.com => 104.16.75.120
	shop.donaldjtrump.com => 104.16.75.120
	www.donaldjtrump.com => 104.16.75.120
Traffic:	

2016-11-28
03:42:32

Case in DNS

DDOS MON

STATISTIC APPLY SIGN IN

Attack Time Line

Detected 0 171.13.38.152 related events in last 24 hours and 37 events in last 30 days.

2016-12-20
09:26:09

IP:	171.13.38.152
Protocol:	DNS
Types:	dns@attack@amp_flood_target
Count:	50
UsedDomain:	cpsc.gov

2016-12-20
05:45:08

IP:	171.13.38.152
Protocol:	UDP
Port:	ALL
Types:	udp@attack@simple_flood_target
Traffic:	

https://ddosmon.net/explore/171.13.38.152

Case in DNS

DDOS MON

DASHBOARD SITES EVENTS | ADMIN HI, XUYANG-PD

Attack Time Line

Detected 0 bsideswim.com related events in last 24 hours and 12 events in last 30 days.

2017-01-08
07:18:37

IP:	23.227.38.32
Protocol:	UDP
Port:	ALL
Types:	udp@attack@amp_flood_target-SNMP, udp@attack@amp_flood_target-NTP, udp@attack@amp_flood_target-TFTP
Chains:	bsideswim.com => 23.227.38.32
Traffic:	

2017-01-06
00:01:12

IP:	23.227.38.32
Protocol:	UDP
Port:	17354
Types:	udp@attack@amp_flood_target-NTP
Chains:	bsideswim.com => 23.227.38.32

https://ddosmon.net/explore/bsideswim.com

Attack Fail Case

ICMP Unreachable (0x0300 - 0x030f)

cpsc.gov\013

How to Solve it

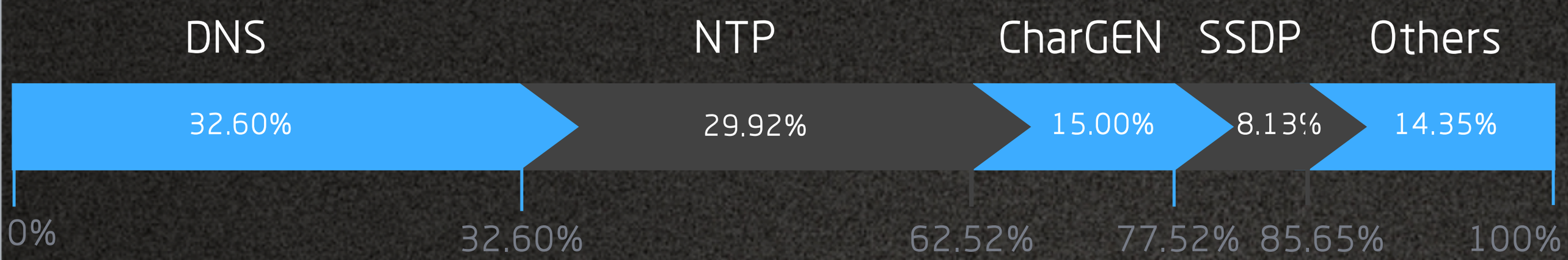
UDP protocol fire and forget trait: like DNS, change to TCP? [1]
IP Spoof: BCP38(RFC2827) [2]
small query & big response:
too many available open UDP amplifier: ?

the combination of these 4 factors

produces a comprehensive vulnerability for the Internet

1. http://www.potaroo.net/ispcol/2013-09/dnstcp.html
2. https://spoofer.caida.org/summary.php

DRDoS Attack Vector



Big Head / Stable Proportion

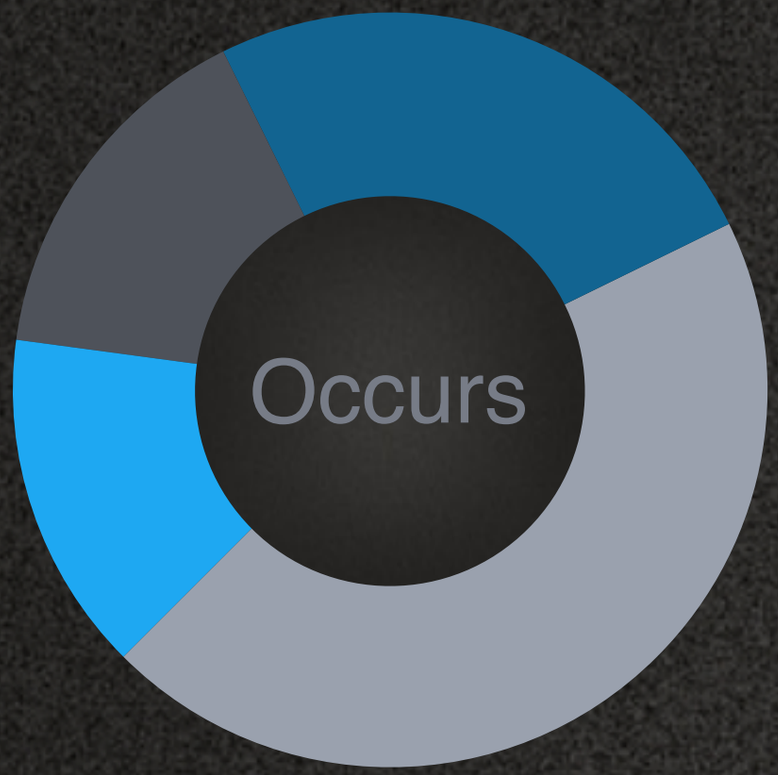
Detection of New Vector, like TFTP / LDAP

DETAILS

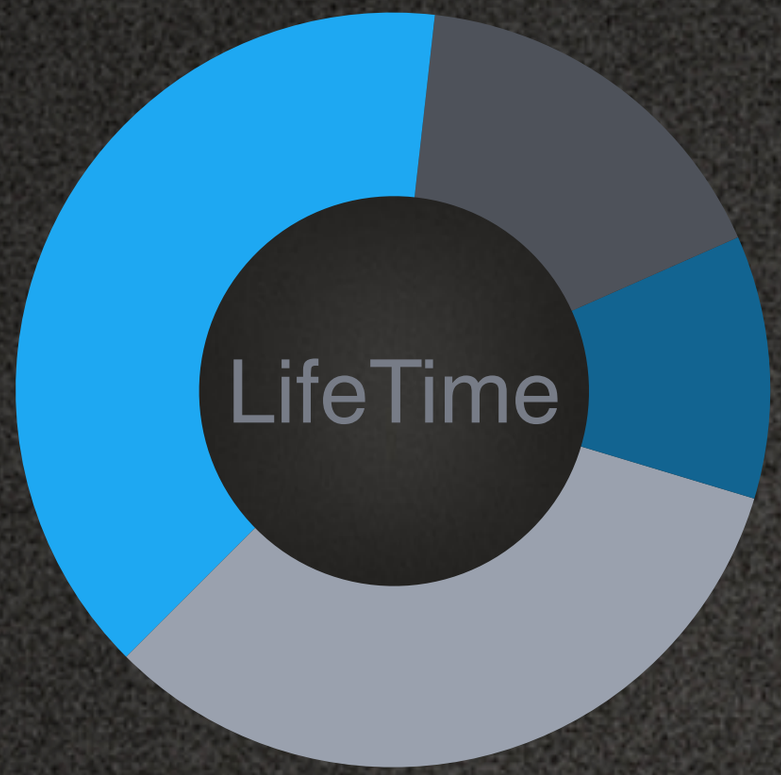
32.60%	32.60%	DNS
62.52%	29.92%	NTP
77.52%	15.00%	CharGEN
85.65%	8.13%	SSDP
87.69%	2.04%	NTP + DNS
89.65%	1.96%	BitTorrent
91.18%	1.53%	L2TP
92.17%	0.99%	NTP + SSDP
93.14%	0.97%	NTP + SNMP
93.99%	0.85%	NTP + TFTP + SNMP
94.74%	0.75%	L2TP + DNS
95.40%	0.66%	SNMP
95.94%	0.54%	NTP + SNMP
96.48%	0.54%	SSDP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

Amplifiers

In Last 6 Months: 100M+ Amplifier Events , 4M+ Unique Amplifier IPs



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



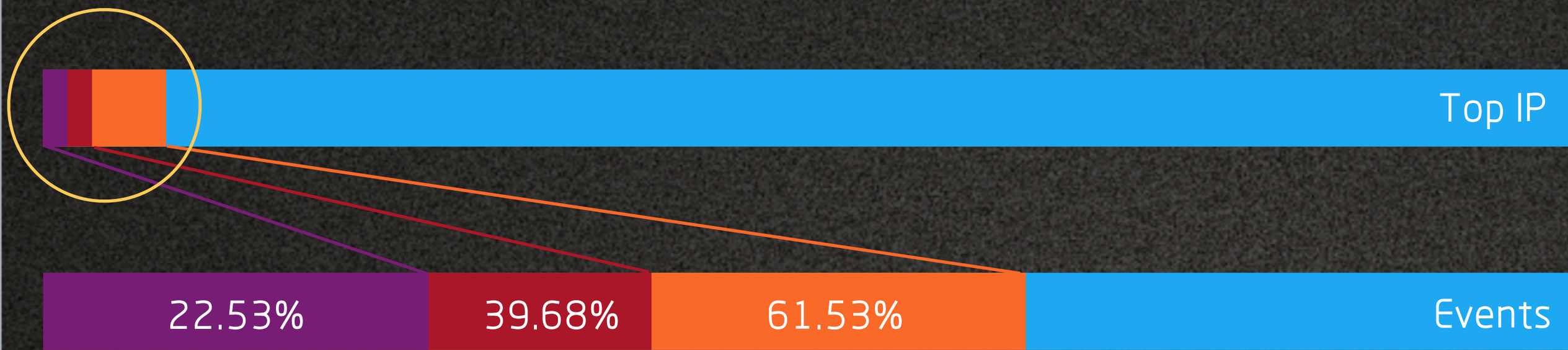
- time <1day
- 1day<=time<1week
- 1week<=time<1month
- time>=1month

DETAILS

Events	Unique IPs	Service
89749356	3928766	SSDP
4860920	58404	NTP
1963505	97375	DNS
787095	9071	CharGEN
517370	9970	Portmap
52162	8858	SNMP
22206	10013	Kad
19067	505	TFTP
12588	4100	mDNS
6444	1804	Others

DNS Amplifier

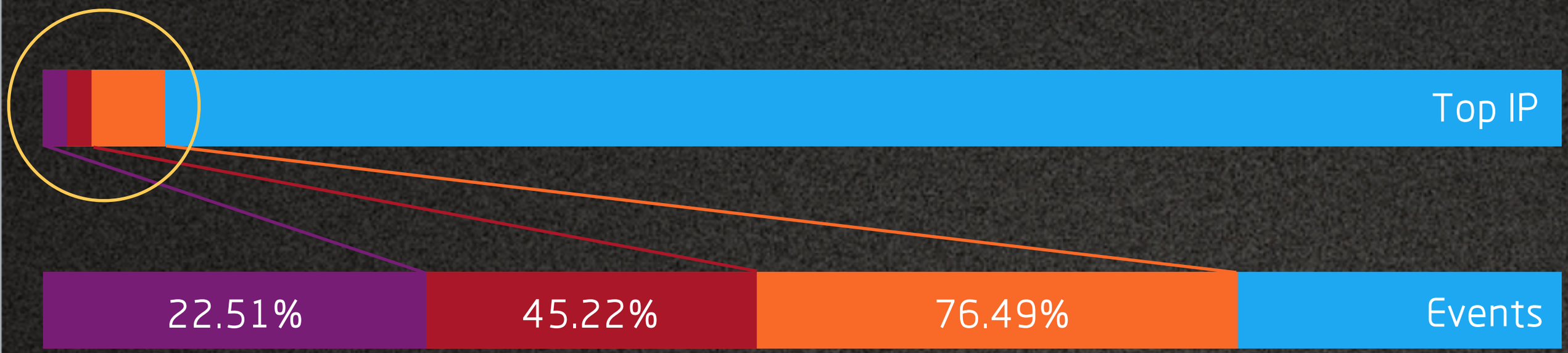
In Last 6 Months: 1.9M+ DNS Amplifier Events , 90K+ Unique Amplifier IPs



	Top Unique IPs	Attack Events	
TOP 1000	1.2%	303088	22.53%
TOP 3000	3.5%	533893	39.68%
TOP 9000	10.5%	827821	61.53%

NTP Amplifier

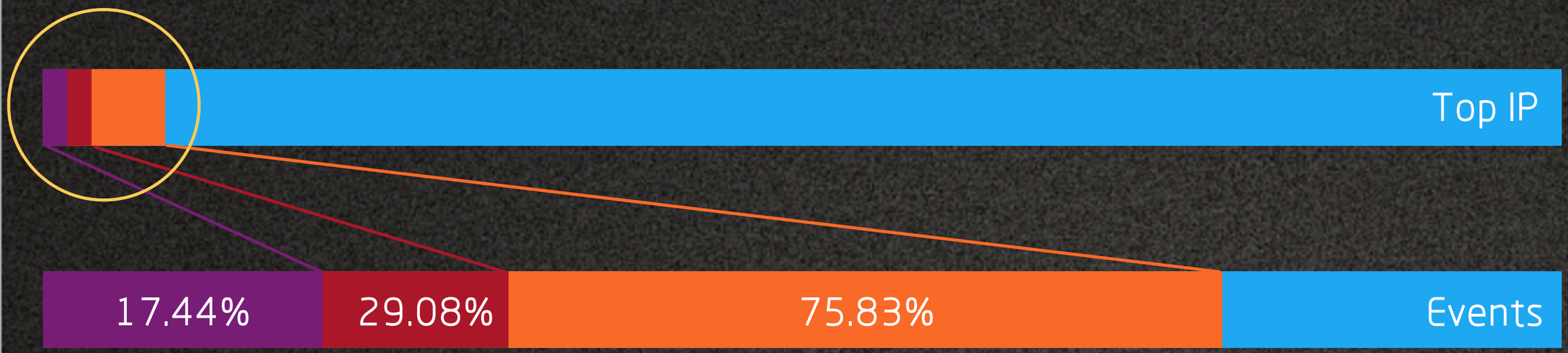
In Last 6 Months: 4.8M+ NTP Amplifier Events , 50K+ Unique Amplifier IPs



	Top Unique IPs		Attack Events	
TOP 600		1.4%	1094077	22.51%
TOP 1800		4.3%	2198121	45.22%
TOP 6000		14.4%	3718307	76.49%

CharGEN Amplifier

In Last 6 Months: 700K+ NTP Amplifier Events , 9K+ Unique Amplifier IPs

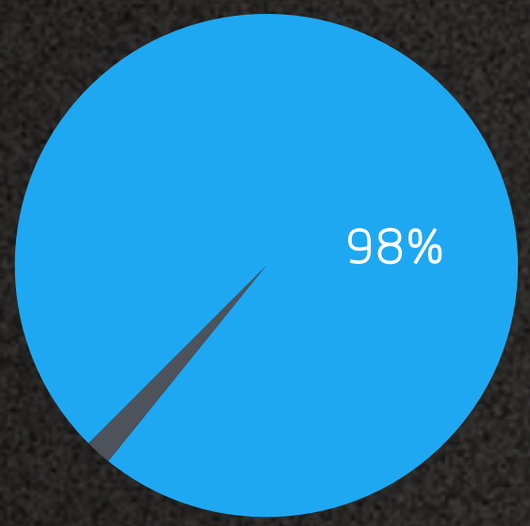


	Top Unique IPs		Attack Events	
TOP 100		1.2%	118568	17.44%
TOP 200		2.4%	197742	29.08%
TOP 1000		12.0%	515587	75.83%

DNS Amplifier

All DNS Amplifier

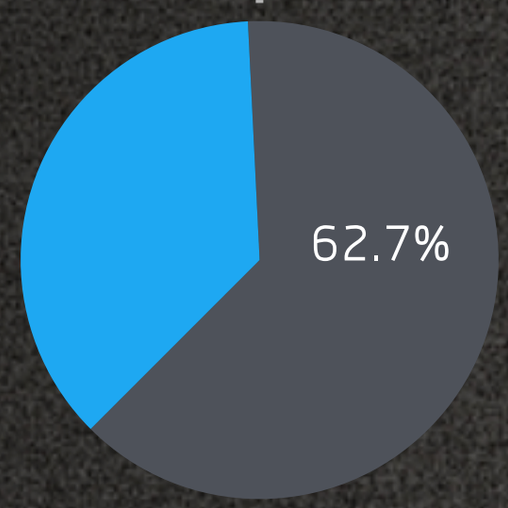
be validated in PDNS data



- Open Resolver
- Abused Authority Server

Open Resolvers

dig @X +time=5 +tries=3 google.com
dig @X +time=5 +tries=3 cpsc.gov



- Live Open Resolver
- "Dead"

"Dead"

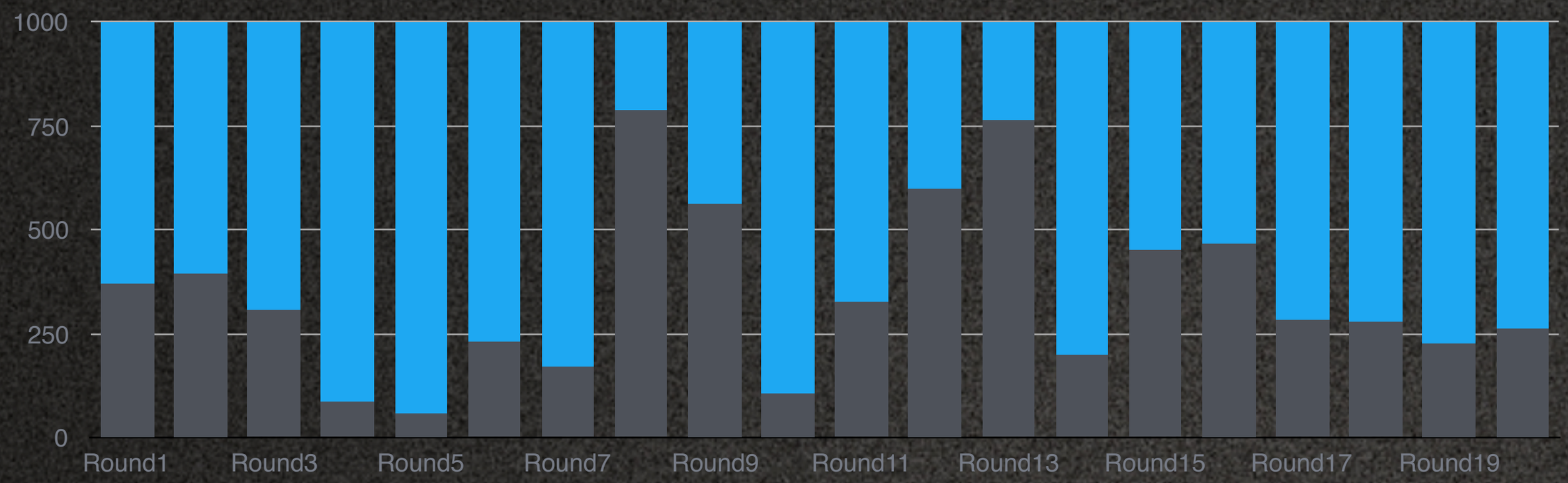
be tagged as "Amplifier" in our real-time DDoS detection system when dig fail
+
re-dig later will success
=
most of them are just be used in attack so heavy that they looks like dead

DNS Amplifier

Test 20 Rounds:

random choose 1000 different amplifiers, in different time

in our real-time detection system to see if it is being used right now



On average, 30% detected DNS Amplifier being used for attack RIGHT NOW

DNS Reflection Used Domain

Almost 100% DNS Reflection Attack are using DNS ANY Query

DETAILS

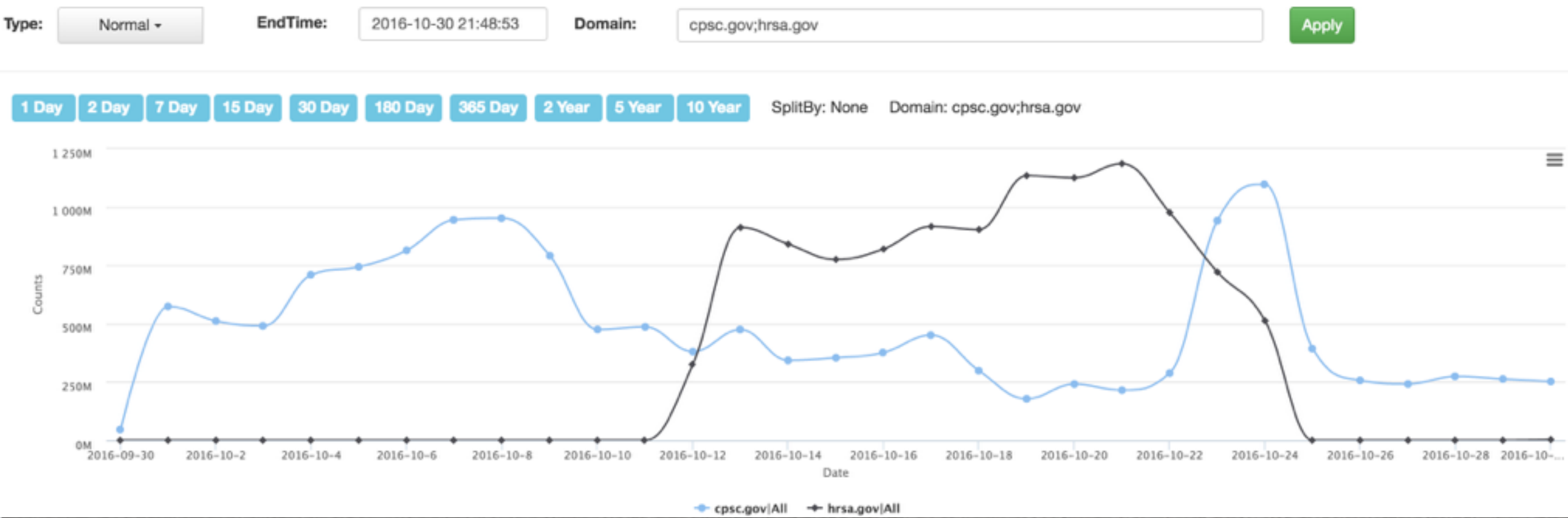
65.25%	65.25%	cpsc.gov
80.22%	17.97%	defcon.org
84.98%	4.76%	aids.gov
88.96%	3.98%	1x1.cz
91.38%	2.42%	kth.se
93.21%	1.83%	nih.gov
94.42%	1.21%	commerce.gov
95.01%	0.59%	isc.org
95.43%	0.42%	wapa.gov
95.77%	0.34%	hoffmeister.be
96.07%	0.30%	doc.gov
96.34%	0.27%	activum.nu
96.58%	0.24%	leth.cc
96.81%	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 Used Domain

dig hrsa.gov any @202.112.51.189 +bufsize=6000



How to Solve it

Amplifier: Kill Top, Kill Half

Used Domain: Kill Top, Kill Almost ALL

1. https://blog.cloudflare.com/deprecating-dns-any-meta-query-type/
2. https://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks/

Further Work

https://ddosmon.net/ // Realtime DDoS attack detection

http://data.netlab.360.com/ // All kinds of open data

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

Will be open:

Daily Active Amplifier

Daily Active DNS Refection Used Domain

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

Thanks


group_info->blocks[0] = grou
else {
for
free_page
out_undo_par
info->bloc
ial_alloc
i >= 0) {