DDoSMon

A Global DDoS Monitoring Project

Ke Qiang, Yiming Gong
Network Security Research Lab, Qihoo 360
netlab.360.com

About

- About 360.com
  - The biggest internet security company in China
  - More than 500 million monthly active Internet users, according to iResearch.

- About us
  - network security research lab, 360
    - Passivedns https://passivedns.cn
    - Scanmon http://scan.netlab.360.com/
    - Opendata http://data.netlab.360.com MalConn, Mirai Sanner, DGA, EK, etc
    - DDosmon https://ddosmon.net
    - And few other projects

Motivation

- DDoS is one of the biggest internet security threat globally
  - Akamai: 129% increase in DDOS attacks in the second quarter of 2016 (*https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q2-2016-internet-security-executive-review.pdf*)
  - Versign: DDOS attacks are becoming more sophisticated and persistent in the second quarter of 2016

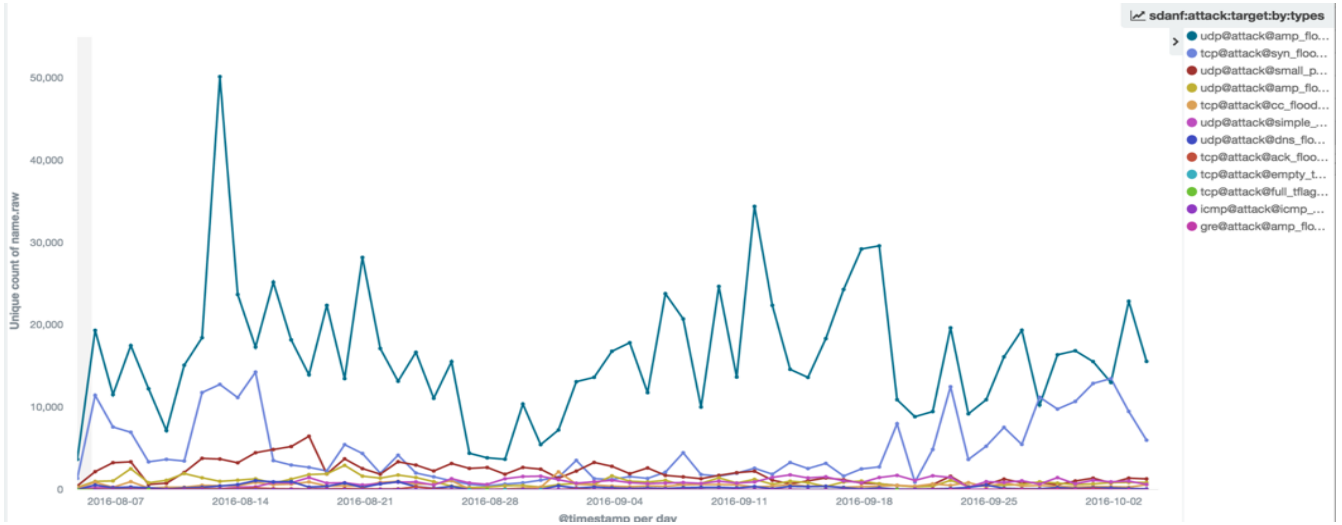
    (*https://www.verisign.com/assets/report-ddos-trends-Q22016.pdf*)

Motivation

- There is a lack of true visibility regarding to DDoS incident
  - ~~Most of the time, only the victims and the big pipe providers know what happen~~
  - For so many events, even the victims or the big pipe providers don’t know exactly what has happened

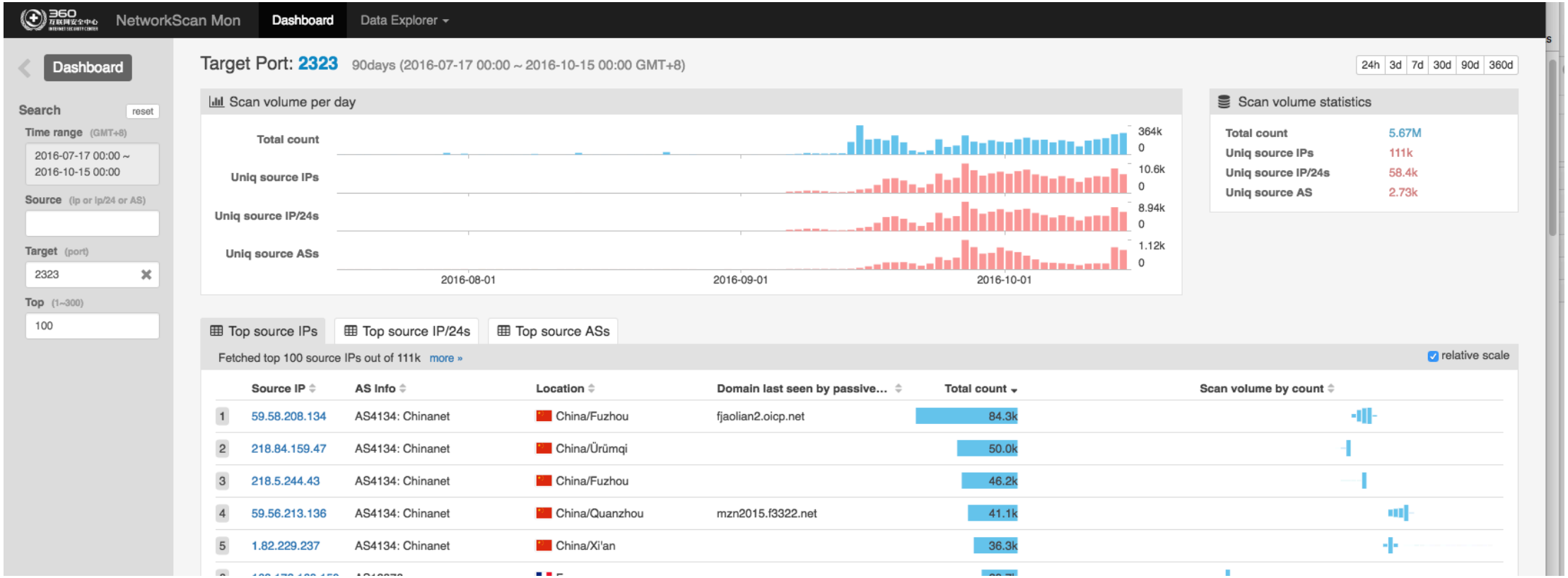
https://ddosmon.net

- On average we see more than 20,000 DDoS attacks every day(one of the biggest?)
- Chances are:
  - If it is a “decent” attack, we are gonna see it, so you can look it up as well



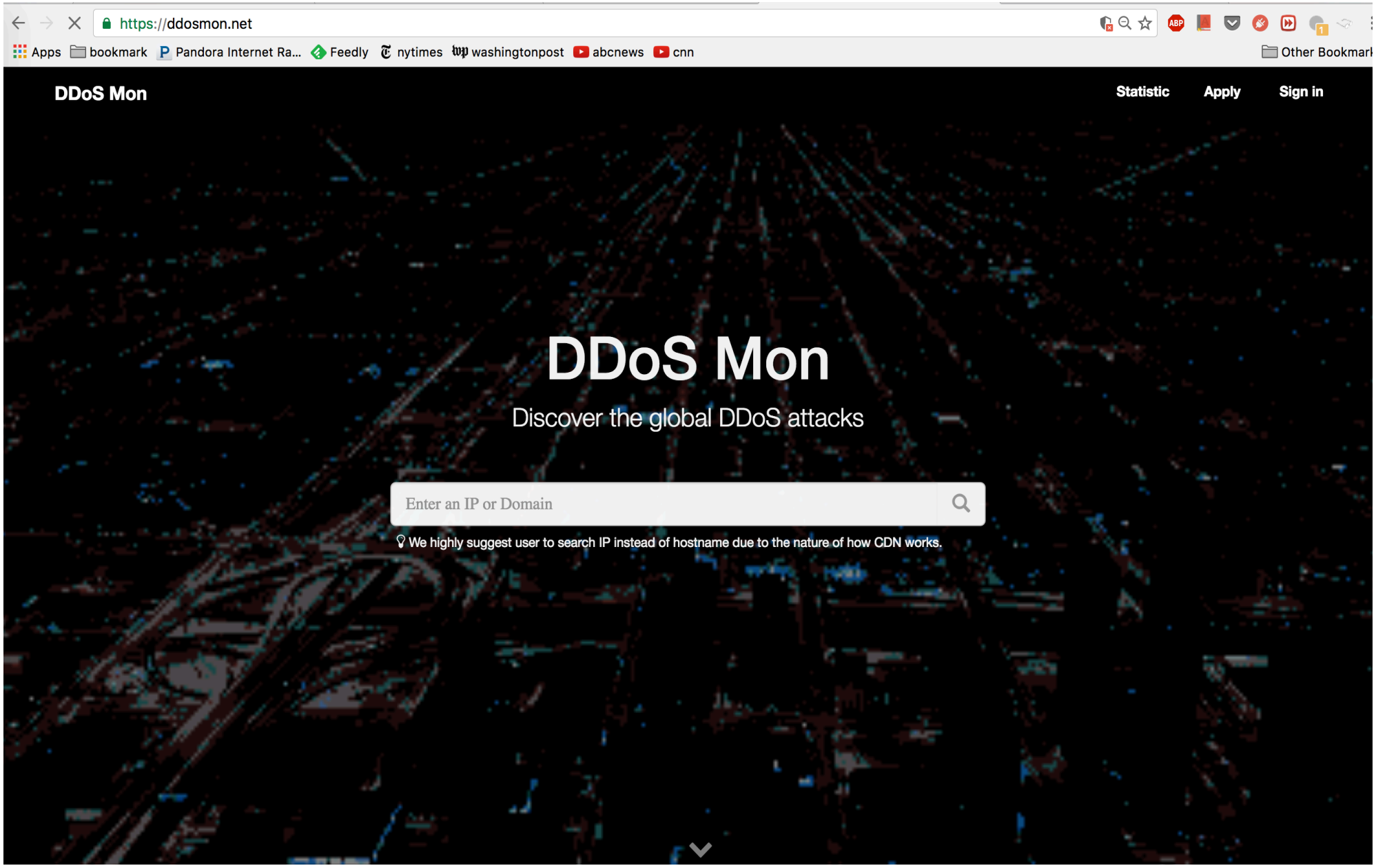
- News: krebsonsecurity.com was under ddos attack on Sep 21

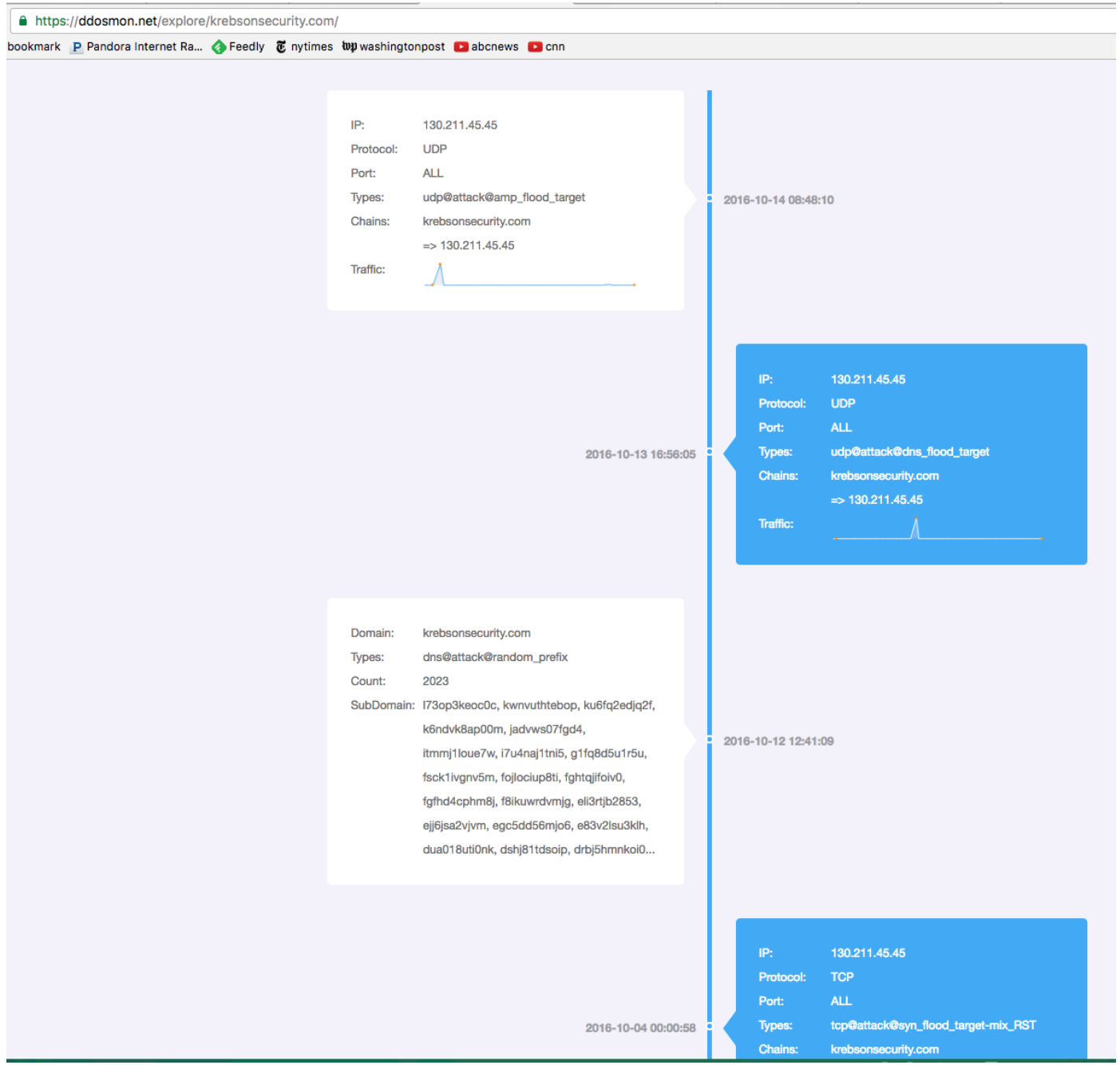
From ScanMon



Our honeypot

```
2016-09-19 17:32:27  INFO: Successful login from 176.35.109.x with credentials admin:123456
2016-09-19 17:32:28  INFO: admin@176.35.109.x entered command: enable
2016-09-19 17:32:29  INFO: admin@176.35.109.x entered command: system
2016-09-19 17:32:31  INFO: admin@176.35.109.x entered command: shell
2016-09-19 17:32:32  INFO: admin@176.35.109.x entered command: sh
2016-09-19 17:32:33  INFO: admin@176.35.109.x entered command: /bin/busybox MIRAI
```


https://ddosmon.net
Apps
bookmark
Pandora Internet Ra...
Feedly
nytimes
washingtonpost
abcnews
cnn
Other Bookmark
DDoS Mon
Statistic
Apply
Sign in
DDoS Mon
Discover the global DDoS attacks
Enter an IP or Domain
We highly suggest user to search IP instead of hostname due to the nature of how CDN works.


https://ddosmon.net/explore/krebsonsecurity.com/
bookmark
Pandora Internet Ra...
Feedly
nytimes
washingtonpost
abcnews
cnn
IP: 130.211.45.45
Protocol: UDP
Port: ALL
Types: udp@attack@amp_flood_target
Chains: krebsonsecurity.com
=> 130.211.45.45
Traffic:
2016-10-14 08:48:10
2016-10-13 16:56:05
IP: 130.211.45.45
Protocol: UDP
Port: ALL
Types: udp@attack@dns_flood_target
Chains: krebsonsecurity.com
=> 130.211.45.45
Traffic:
Domain: krebsonsecurity.com
Types: dns@attack@random_prefix
Count: 2023
SubDomain: l73op3keoc0c, kwnvuthtebop, ku6fq2edjq2f, k6ndvk8ap00m, jadvws07fgd4, itmmj1loue7w, i7u4naj1tni5, g1fq8d5u1r5u, fsck1ivgnv5m, fojlociup8ti, fghtqjifoiv0, fgfhd4cphm8j, f8ikuwrdvmjg, eli3rtjb2853, ejj6jsa2vjvm, egc5dd56mjo6, e83v2lsu3klh, dua018uti0nk, dshj81tdsoip, drbj5hmnkoi0...
2016-10-12 12:41:09
2016-10-04 00:00:58
IP: 130.211.45.45
Protocol: TCP
Port: ALL
Types: tcp@attack@syn_flood_target-mix_RST
Chains: krebsonsecurity.com

DDoS Mon

Dashboard | Sites | Events | Admin

Victim IP: 130.211.45.45

Attack Time: 2016-10-12 12:43:44

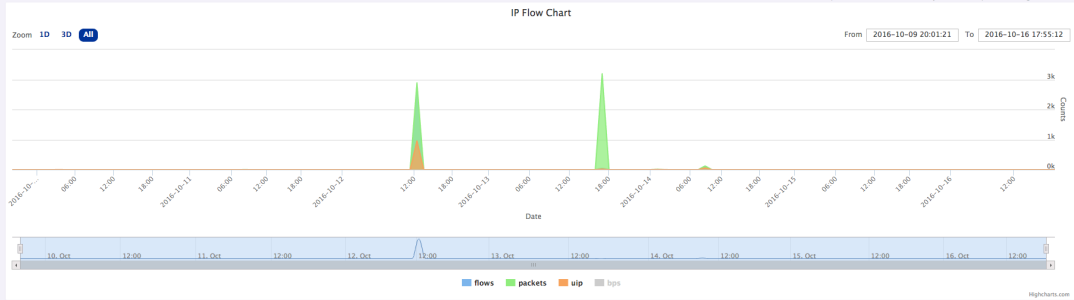
Possible Type: traffic spike

DNS Snapshot

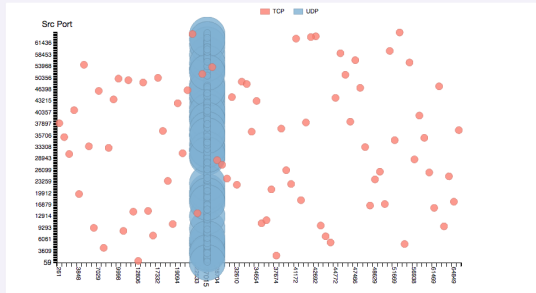
Domain	CNAME	IP
krebsonsecurity.com		130.211.45.45, 2016-10-12 12:12:27

IP Flow Chart

There might be some delay for the data to be displayed after you get an alert, please check back in 30 mins if you don't see spike in the diagram.



Src-Dst Port heatmap



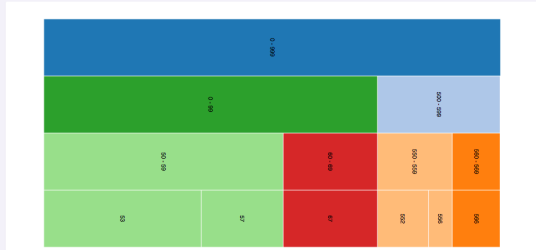
Top Src Port

SrcPort	Flows	Protocol	BPS	PPS	Percent
42763	2	UDP,TCP	30	0	0.1%
62830	2	UDP	6	0	0.1%
30671	2	UDP	6	0	0.1%
53763	2	UDP,TCP	30	0	0.1%
45364	2	UDP,TCP	30	0	0.1%

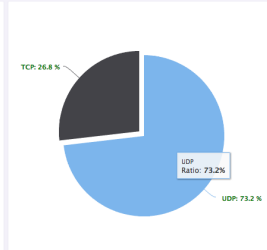
Top Dst Port

DstPort	Flows	Protocol	BPS	PPS	Percent
27015	1911	UDP	5526	95	72.0%
13321	2	TCP	55	0	0.1%
46858	2	TCP	55	0	0.1%
28688	2	TCP	55	0	0.1%
33555	2	TCP	55	0	0.1%

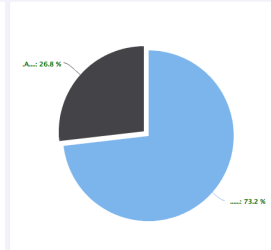
Bytes Distribute



Protocol Distribute



Flags Distribute



Top Src IP

SrcIP	Flows	Protocol	BPS	PPS	Percent
120.70.15.223	168	UDP,TCP	949	8	6.3%
117.25.202.61	83	UDP,TCP	1450	4	3.1%
121.206.59.13	69	UDP,TCP	1054	3	2.6%
219.150.151.164	63	UDP,TCP	366	3	2.4%
120.37.132.204	53	UDP,TCP	400	2	2.0%
218.67.72.11	53	UDP,TCP	500	2	2.0%
218.86.89.249	53	UDP,TCP	476	2	2.0%
222.79.222.9	49	UDP,TCP	439	2	1.8%
120.43.228.190	46	UDP,TCP	430	2	1.7%
49.119.177.229	44	UDP,TCP	191	2	1.7%

What else?

- Botnet command tracking system
  - We have even more interesting finding there regarding to Miari
- Mirai-bot IP download
  - http://data.netlab.360.com/mirai-scanner

How does DDoSMon Work?

- Mainly based on three major components
  - Realtime NetFlow traffic (layer3)
  - Realtime DNS traffic(DNS amp, DNS reflection..etc)
  - Realtime DDoS botnet command tracking system

1: Realtime NetFlow Traffic

- Collect huge volume NetFlow from various networks
  - Large network backbone routers
  - User contribute flows

- Handle more than 30 billions NetFlow records every day
- Data is processed in near real-time

NetFlow Based Attacks Detection

Spike detecting

The first important step for the heuristic DDoS attacks recognition

- Establish baseline for all the IPs
- Detecting anomaly traffic spike in realtime
- Utilize cumulative moving average algorithm

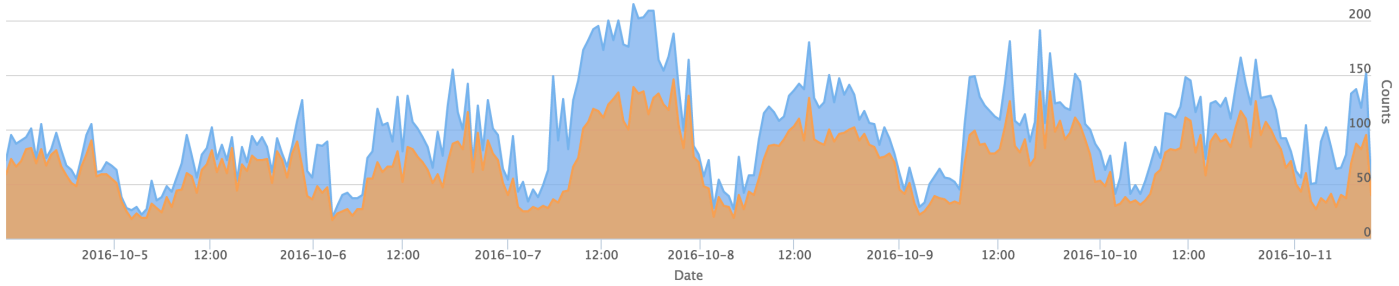
Characteristics recognition

Different DDoS attack vectors usually presents a certain characteristics on NetFlow traffic.

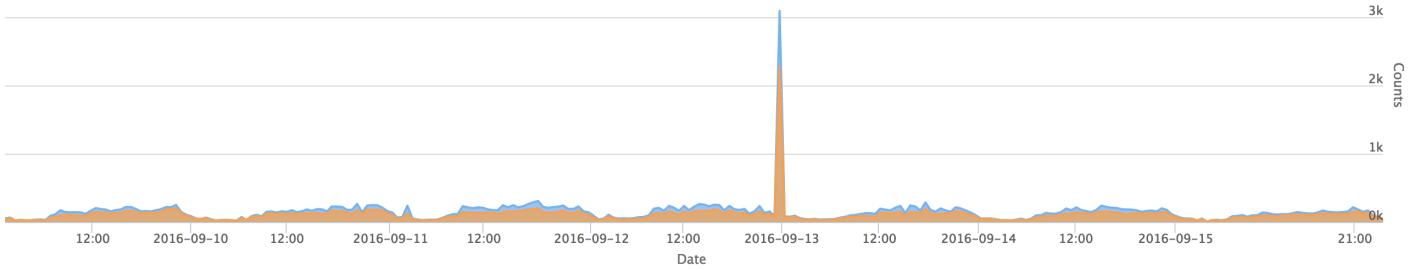
- UDP Reflection flood
  1. More than 90% traffic is UDP
  2. Most of the packets from some fixed suspicious source port e.g. 19, 53, 123, 1900, 0
  3. Most of the packet has large bytes
- SYN flood
  1. More than 90% traffic is TCP
  2. All TCP Flags only has SYN Flag set packets
  3. Source IP address distribution normally not enough random

- We use the attack against www.bankofamerica.com (171.161.199.100) on Sep.14 as an example to illustrate

Spike Detecting



The traffic figure for 171.161.199.100 from 2016-10-05 to 2016-10-11



The traffic figure for 171.161.199.100 during attack happen(2016-09-09 to 2016-09-15)

- An obvious spike can be observed from NetFlow perspective during attack happen.

Characteristics recognition

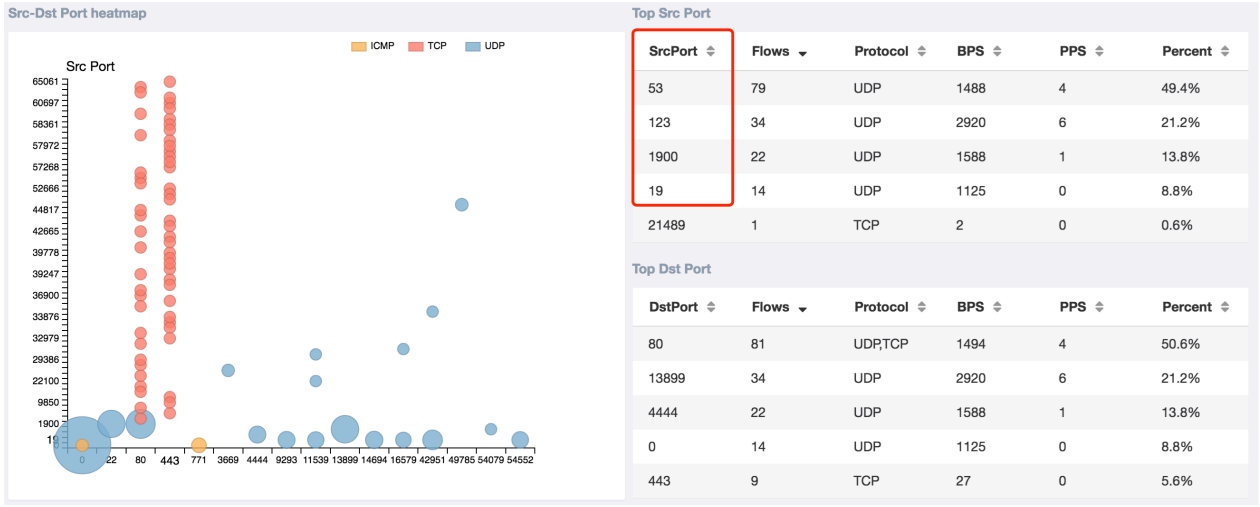
- UDP reflection amplification characteristics can be observed from NetFlow records at the attack target BOA

```
kenshin@MacBook-Pro Downloads$ flame 'dst ip 171.161.199.100' --start="2016-09-14 10:00:00" --end="2016-09-14 14:00:00"
Date flow start     Duration     Porto    Src IP Addr:Port              Dst IP Addr:Port       Flags    Tos    Packets Bytes
2016-09-14 12:37:58      16      UDP      219.141.149.59:123      ->    171.161.199.100:17928  ......   0      2       936
2016-09-14 12:46:13      15      UDP      59.44.147.62:1900       ->    171.161.199.100:80     ......   0      2       682
2016-09-14 12:45:14      0       UDP      1.180.64.218:1900       ->    171.161.199.100:80     ......   0      1       320
2016-09-14 12:11:41      9       UDP      218.84.36.106:19        ->    171.161.199.100:54552  ......   0      2       3000
2016-09-14 12:46:12      0       UDP      59.44.155.238:1900      ->    171.161.199.100:80     ......   0      1       316
2016-09-14 12:49:30      0       UDP      115.183.24.122:1900     ->    171.161.199.100:80     ......   0      1       338
2016-09-14 12:37:57      25      UDP      124.239.183.6:123       ->    171.161.199.100:63456  ......   0      5       2410
2016-09-14 12:38:11      20      UDP      27.191.225.23:123       ->    171.161.199.100:1972   ......   0      2       936
2016-09-14 12:11:44      0       UDP      59.44.155.238:1900      ->    171.161.199.100:22     ......   0      1       354
2016-09-14 12:15:49      0       TCP      1.82.216.134:31631      ->    171.161.199.100:80     ....S.   0      1       52
2016-09-14 12:49:12      23      UDP      27.191.146.242:1900     ->    171.161.199.100:80     ......   16     2       614
2016-09-14 12:37:42      63      UDP      124.239.183.6:123       ->    171.161.199.100:17928  ......   0      16      7712
2016-09-14 12:52:31      0       UDP      27.191.156.66:1900      ->    171.161.199.100:80     ......   0      1       270
2016-09-14 12:42:31      0       UDP      27.191.237.6:1900       ->    171.161.199.100:80     ......   0      1       354
2016-09-14 12:36:30      58      UDP      124.239.183.6:123       ->    171.161.199.100:54079  ......   0      20      9640
2016-09-14 12:38:08      37      UDP      124.239.183.6:123       ->    171.161.199.100:54079  ......   0      7       3276
2016-09-14 12:56:12      0       UDP      59.47.40.28:1900        ->    171.161.199.100:80     ......   0      1       334
2016-09-14 12:37:06      27      UDP      106.46.133.72:123       ->    171.161.199.100:1972   ......   0      3       1446
2016-09-14 12:37:31      22      UDP      27.191.225.23:123       ->    171.161.199.100:39209  ......   0      2       936
2016-09-14 12:50:37      0       UDP      27.191.236.5:1900       ->    171.161.199.100:80     ......   16     1       300
2016-09-14 11:56:17      0       UDP      220.181.65.227:53       ->    171.161.199.100:4444   ......   0      1       1500
2016-09-14 12:10:09      27      UDP      36.110.119.48:0         ->    171.161.199.100:0      ......   0      3       3343
2016-09-14 11:56:09      0       UDP      61.150.96.247:1900      ->    171.161.199.100:80     ......   0      1       334
2016-09-14 12:10:41      0       UDP      61.178.176.144:1900     ->    171.161.199.100:22     ......   0      1       270
2016-09-14 12:18:35      0       TCP      123.206.29.139:39321    ->    171.161.199.100:443    .A....   0      1       52
2016-09-14 12:35:48      0       UDP      106.39.244.204:123      ->    171.161.199.100:63903  ......   0      1       468
2016-09-14 12:50:58      0       UDP      111.225.206.245:1900    ->    171.161.199.100:80     ......   1      1       310
2016-09-14 12:41:57      0       UDP      61.178.139.19:1900      ->    171.161.199.100:80     ......   0      1       354
2016-09-14 12:36:47      0       UDP      219.147.159.2:123       ->    171.161.199.100:55493  ......   0      1       468
2016-09-14 12:47:33      0       UDP      61.134.67.139:1900      ->    171.161.199.100:80     ......   16     1       270
2016-09-14 12:41:00      0       UDP      113.140.50.194:1900     ->    171.161.199.100:80     ......   0      1       342
```

The raw NetFlow records of 171.161.199.100 during attack happend

Characteristics recognition – Source Port

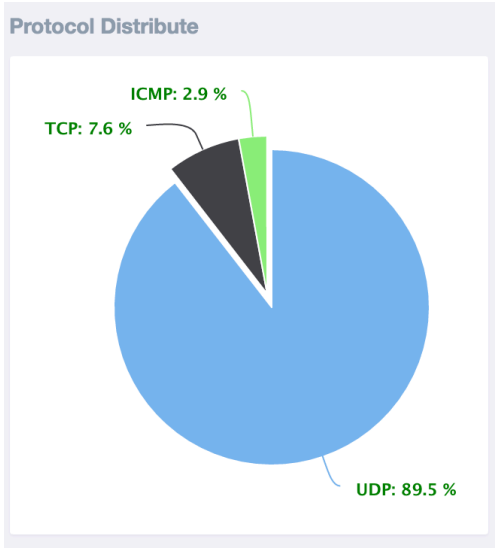
- Most of the packets from suspicious source port
  - UDP port 53 DNS reflection DDoS
  - UDP port 1900 SSDP-based DDoS
  - UDP port 123 NTP-based DDoS
  - UDP port 19 Chargen-based DDoS
- Mixed mulitiple attack vectors



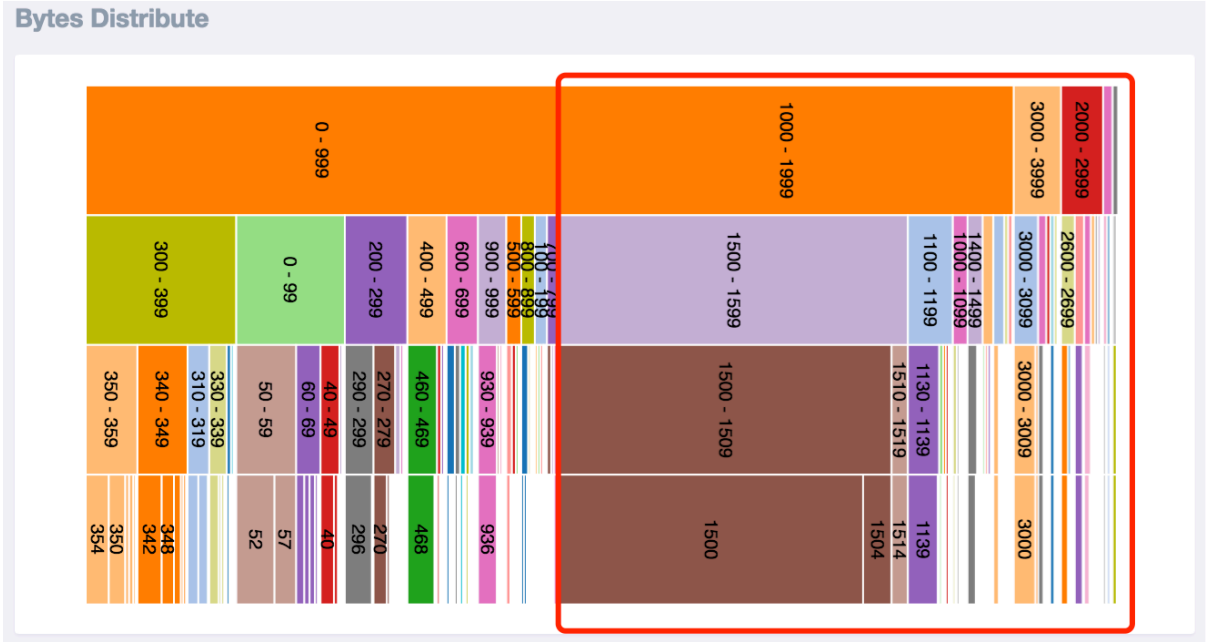
The source & destination port statistic page screenshoot

Characteristics recognition – Protocol &Packet Size

- UDP packet percentage is unusually highly compare to normal WEB traffic
- Packet size is unusually large, plenty of the packet sizes are 1500 bytes reaching MTU threshold



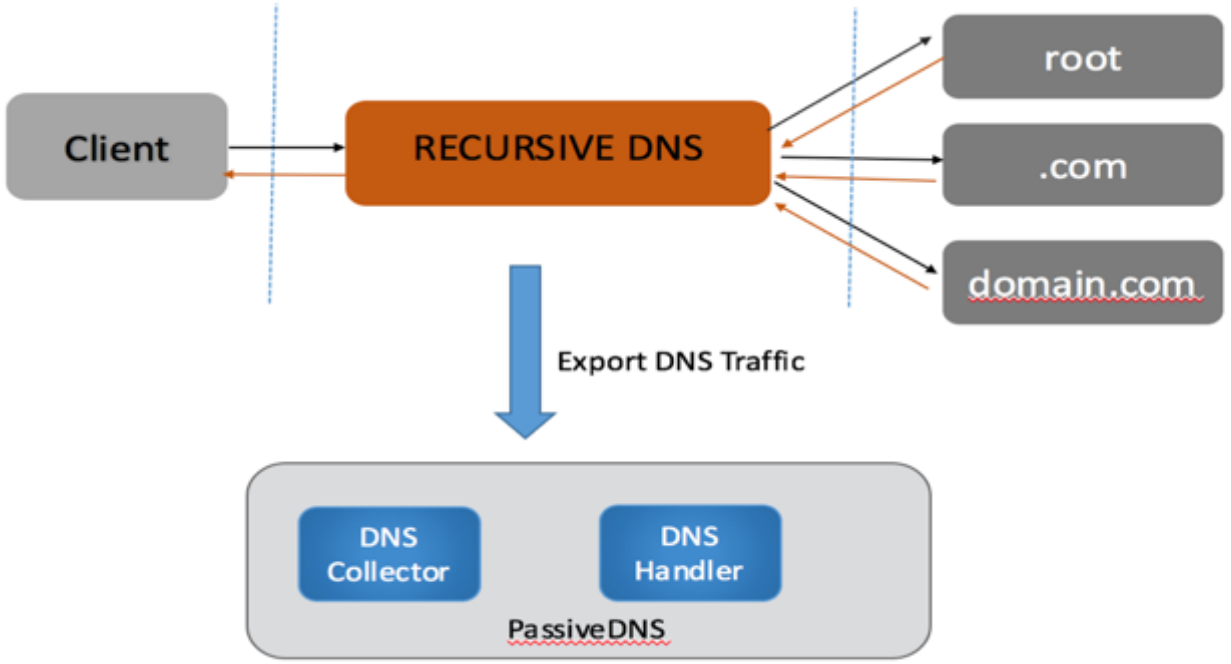
The protocol statistic screenshoot



The packet size statistic screenshoot

2: Realtime DNS Traffic

- Process 240 billions DNS requests every day which covers about 10% total DNS traffic in China
- We also operate a Passive DNS platform https://passivedns.cn

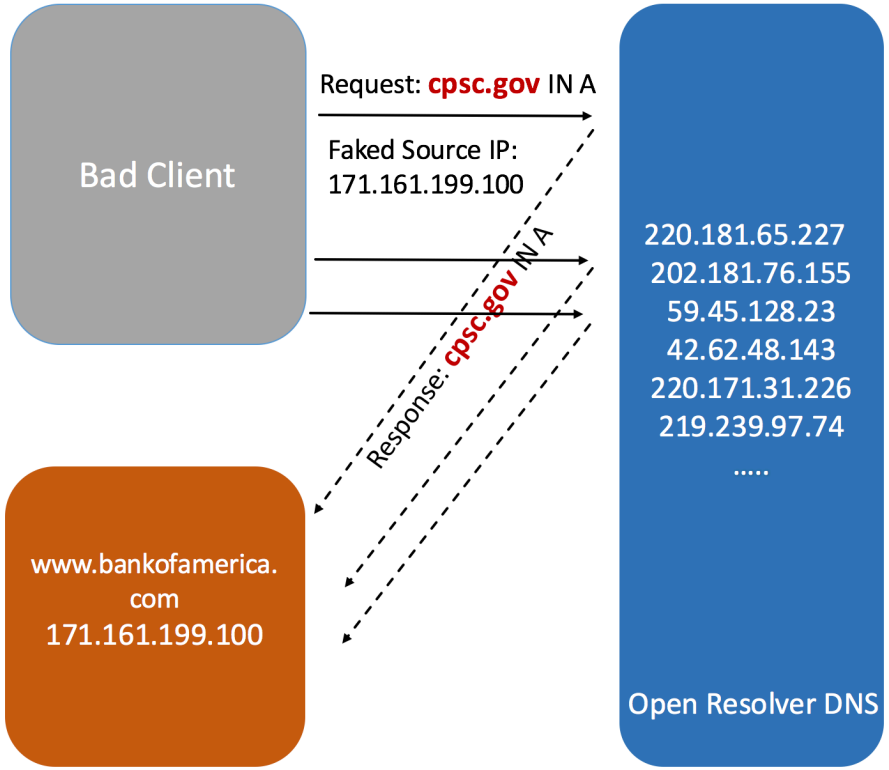


Realtime DNS Traffic

- What can we get from DNS traffic?
  - The ability to monitor Domains instead of just IPs.
  - DNS reflection/amplification attacks
  - Random subdomain attacks

Realtime DNS Traffic – DNS reflection/ amplification attacks

- Again use the example of BOA
- How it works
  - cpsc.gov was abused
  - Attacker uses BOA address as query source to ask lots of open dns resolvers for cpsc.gov
  - The dns responses from the open resolvers flooded BOA address



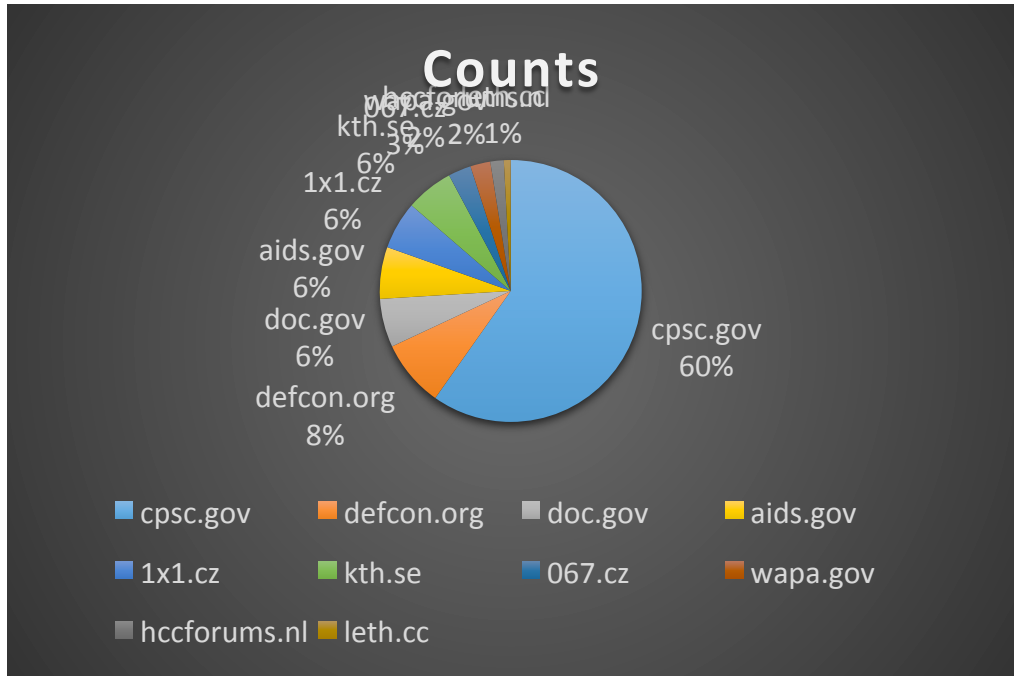
Realtime DNS Traffic – DNS reflection/ amplification attacks

- Why is cpsc.gov?
- $ dig cpsc.gov any +tcp

```
kenshin@li817-198:~$ dig cpsc.gov any +tcp

; <<>> DiG 9.8.1-P1 <<>> cpsc.gov any +tcp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27368
;; flags: qr rd ra; QUERY: 1, ANSWER: 22, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;cpsc.gov.                      IN      ANY

;; ANSWER SECTION:
cpsc.gov.               18690   IN      SOA     auth00.ns.uu.net. hostmaster.uu.net. 994725 1800 600 1728000 21600
cpsc.gov.               18690   IN      RRSIG   SOA 7 2 21600 20161014030500 20161007020500 10037 cpsc.gov. Z1Y0HVBLLOGGhlEPfufuGFm2RZH2MOqbBdDfqMsMDbBcWJp1T8fKVhJb bDRd5prXfBEKYZWNc7TZozCYUEsfrx4o
9Y9NrT9iHtpKuqTH3jeGMDEN MQp9Qc9CEIdU2yswmjaiYc8MGEkBpzwRPVrcYcaYuc9DGDFSeMEnV+0v KvFMfxEFrvg+3mgIhziU+xhizHVM6E53NObZqpKs+Fr+lgpTvxqM5//O hllEruVekCnwsGs7GCKCiBdDR3WLK0Q/GAfYfHwUOeEcItvRv0O53pHf Y
B5MpZ4HBKdMiMJqhYATSuriAEt0kRpecqc1s/+XJ6Hv2RgAwGC7Q8B2 TdSIPw==
cpsc.gov.               18690   IN      NS      auth00.ns.uu.net.
cpsc.gov.               18690   IN      NS      auth61.ns.uu.net.
cpsc.gov.               18690   IN      RRSIG   NS 7 2 21600 20161014030500 20161007020500 10037 cpsc.gov. BESyMvlElwMoL8m9M6EjgTgYRVtQefVQMskpikjzu2z1hyoEyy3z8Ib7 gHtHd75hPfZ3XEk5GeY8DRn5jp/09wGZh
0bbFxsf6jMYGYZyuPwqsujw +xYXhIghPXTdXeyhHtGo8p8MVKy7YRzr2LKuga4VnpsNcM9JNTqJqGu1 DuS5RVPn8qD5IUksFsLYUDF+Qd0ozb+Kfa0wXIgkOUwkA+yPguie1UnT YqBidnCEF9QR0KoP5Z4lDUrzHietXZ5oZgmglmSuGyK8ZliSm/l5cb7p vn
Nu4ho7SCLXuQ9I1GMU5MJWwZSTjgZZnmkyB27pnTt8Imhmfh0i1qmA e0Ecqw==
cpsc.gov.               18690   IN      NSEC3PARAM 1 0 12 AABBCCDD
cpsc.gov.               18690   IN      RRSIG   NSEC3PARAM 7 2 21600 20161014030500 20161007020500 10037 cpsc.gov. BTWgDsh5G0kt9Qga5F+Tm8HgCConhoyE5Ni4CwRkl6dFrz8KobQ7PI8T UkfqrF1M1Wed27P2rcVkqd59I
8fZDWGvK/7icP8hchOLuFBP43KRzKD+ mmjnN47slZTihzBlFzrAcO5h0fiyE2bOYFXdWUm/gLdlyCNYAB7cqTA2 Vx9H2aqWzu6Iqo0TTuP1Ef7ADouOGd6xFgSzZlXoKQ+Z2oad/kV64DVQ SksoEgEZNbiIU3dUfN/LwRL/7A9NQkIfUa4GoIZJw6T1W0MFhae
mHi+o nUk8Q1lL8JENmWorAmweTbl1uqxiyhbM5ffyRd08+u5zBCxIKpaltfsj +Rmy6w==
cpsc.gov.               18691   IN      DNSKEY  256 3 7 AwEAAXbON5mPbmV6NQthq+jKiviTwb7VXv8Ni5dpsfLtDanWA/RfTiIS APXMX14/odFFEBNVGcJSlft5cy7w5iPCzptecMogt51mDJVRB9oJMPW/ 1Ki3SeXMx1Fh3uV10jkPhvNbPTm
FY8wWepRJagjnXgnyRx2hGnP6EAnQ fYrBJ51gEUtBYeQvfuvnhbhXr4zIVIjFelde/AE29wWpRhIA+cv3+7P2 0yx8A5Iut+35Hvp3x8ku9dNCr/Nkw+wGt/XwXf2Z0Kr9lDHIdG6BxyBf vwrCM7LJvY7s84fVuUFM3R9q0VyISQWZvKphCIwJRd/e4nTZb1buS
cW3 sy4yX5oe/zk=
cpsc.gov.               18691   IN      DNSKEY  257 3 7 AwEAAX5Tor9V7TnhfUMAL67reT+IFYd+4ciQv/UnvZbNgj7DgDuJPpcl Owh6ypAldCYgTXkF2Qt+an9WVp+Khsp2wRCCOhvGIUR9sOGdzxumDUCT Uru2dxHAqIn1QYSjuT8huMDDyBJ
mnoA4AY1Te86mcE1Jwpo+S9KoB23Z JgnMedU+6i8Qm9cdGLNM7nqEXhgKgmKc/387UFdh25jltsg0d2gOK//q k2HfLdDqv8Xlrlacf MsSXniVwK7E6mtqcfbF518M2bl6UFJWXuxp+cU8 0WdmGiQfxmLvm62a2aVs9IzR6qGg0Ce5bxbx68v6gYTgIOUBm8ERy
tZ3 T2jzc0QOKQc=
cpsc.gov.               18691   IN      DNSKEY  256 3 7 AwEAAepXgcviRvTWTMcZ4MjFIZe/plj2y6gkDQf0GTgc3mb/UznTvAsu 2ABKSTLxKSLSsVXfSXVBwSSHS3d91My1B8QUf9Z2Uq0PpDR91ALH6KHm apiDwI+IBDIlzT2XNC7QYaqHp8J
vxeOLUf2i/PWIB5w7NlYHbt0NF+sg wSPm34eTpqRDQUCKp3DwmlzTwnb54Wk2wQC3ZosFZtJZ5H+LaRjTbS3k y6GPY0wB6C+2z27fiR0rtPd3uGNQKIVu0qrUatZAj4Lr6HE9CkD8PVQF 7QC+k+/MdoKVmKRyX3SL6TJBq5PbgMS/VOJEmYwx/4aXBADd4Bk1Y
W+u Ijl84w4DB5s=
cpsc.gov.               18691   IN      DNSKEY  257 3 7 AwEAAZztz17cVspxUk8egfYEFLuyPXVETlPdT2PAuy+cZTk3afTS7cda Tnsk43AIqgnCkTvHE9m4gVuOhNmFjPIABPkfmaCtOzyqVmLjxb36JMxJ TnhBPBYjWY0HrBdEGCGG7eZzY4l
l9kAMPIxE1OmMl9iM0dQSzamITEWN 89oPptHnlbjz8k7nQO3xyzXreamjhIW/2iIJhM+CdHe2CgMhPtf8b4QR 8CuIBMH07gvsTKljuvQLiS1ThQYYpmLgriiWjnQFum2FJe6J7x8joDAq YCzbQUdGSyJPp6FYibaG70Y62fIf9DNgHRMH/3c79DW9RmwzFgggjf
KLf y4hOgRbsVFc=
cpsc.gov.               18691   IN      RRSIG   DNSKEY 7 2 21600 20161014030500 20161007020500 10037 cpsc.gov. MukWlU+TWEevamxMW+d5HYDEUrSO2xWwUd7mKXPVG0aCzJ1n67gAAU4h rZcm3HnO3QO1CclEzffJdmONn+nec
vkt1Vr1XUZLDm3I6H5eqSgV1baR MmovhUVe3r41Pq87IvmUKjjtjw1S8acLKAdFA0yq5MSxiwRrXhXSFtj4 lvesKRsUKgzGPcypHjYh5Y7ElI5wNsv4BjR4OD6sZhIZIOMF95BBkpty khJhnshgN9Ae5TGuk+G7EEZS+KWwPMF2E2qj+y0gTa5NBIQjD6Rws/S
L p0mv6NNm1XP5yeMWDnuZhOGiVEFWsPrPRUyOLIAeKe12vatcErHN2UVH tl7wsw==
cpsc.gov.               18691   IN      RRSIG   DNSKEY 7 2 21600 20161014030500 20161007020500 58273 cpsc.gov. Z04LdPeBCeJkUJvTnPgzV8g0aeNOkfZuEly8KlSyu0xw9NuHSkNXLouB 7aCnNuiEI0N/lV+ofm3on9uX9vKIr
NqyHyPujlE9n8dQL3A5kmewlYx5 aCcfKovpEO5w3DW0o/qRlraBgYbFku2YjR2kst6siLrWW71sUGkH1JX0 af6P1TOzCCV+s1jse+A9rzvOGM3Slz2mJtqnYg1foPjtWrBsG4HQmoMV qbPooLis7yXuTTb4ulIiIvz4G+wqZsYSIQ+pEPfohBOk2fgfcLmB0Ms
o MrUXhck1Goe1glllcS2EYqdFnj04WsUH00qh/07YpppZESyWkC7WviEv AUXCvQ==
cpsc.gov.               18690   IN      AAAA    2600:803:240::2
```

Realtime DNS Traffic – DNS reflection/ amplification attacks

Top abused domains



Live data

Datetime	Victim	UsedDomain
2016-10-08 00:10:14	184.75.209.236	defcon.org
2016-10-08 00:10:14	185.128.40.162	defcon.org
2016-10-08 00:10:14	90.208.201.165	defcon.org
2016-10-08 00:10:12	178.188.81.218	leth.cc
2016-10-08 00:10:12	213.209.90.198	kth.se
2016-10-08 00:10:12	74.213.89.192	kth.se
2016-10-08 00:10:10	103.58.149.181	cpsc.gov
2016-10-08 00:10:10	108.231.116.136	cpsc.gov
2016-10-08 00:10:10	158.69.4.72	cpsc.gov
2016-10-08 00:10:10	167.114.43.64	cpsc.gov
2016-10-08 00:10:10	185.109.62.178	cpsc.gov
2016-10-08 00:10:10	192.95.56.216	cpsc.gov
2016-10-08 00:10:10	157.228.66.136	cpsc.gov
2016-10-08 00:10:10	203.75.190.22	cpsc.gov
2016-10-08 00:10:10	203.69.23.216	cpsc.gov
2016-10-08 00:10:10	209.222.104.60	cpsc.gov
2016-10-08 00:10:10	216.58.192.112	cpsc.gov
2016-10-08 00:10:10	78.199.64.208	cpsc.gov
2016-10-08 00:10:10	89.84.116.77	cpsc.gov
2016-10-08 00:10:10	93.169.188.78	cpsc.gov
2016-10-08 00:10:10	80.1.218.158	cpsc.gov
2016-10-08 00:10:09	178.188.81.218	1x1.cz
2016-10-08 00:05:12	184.75.209.236	defcon.org
2016-10-08 00:05:12	185.128.40.162	defcon.org
2016-10-08 00:05:12	31.220.41.13	leth.cc
2016-10-08 00:05:12	74.213.89.192	kth.se
2016-10-08 00:05:11	78.179.66.230	dyn.com

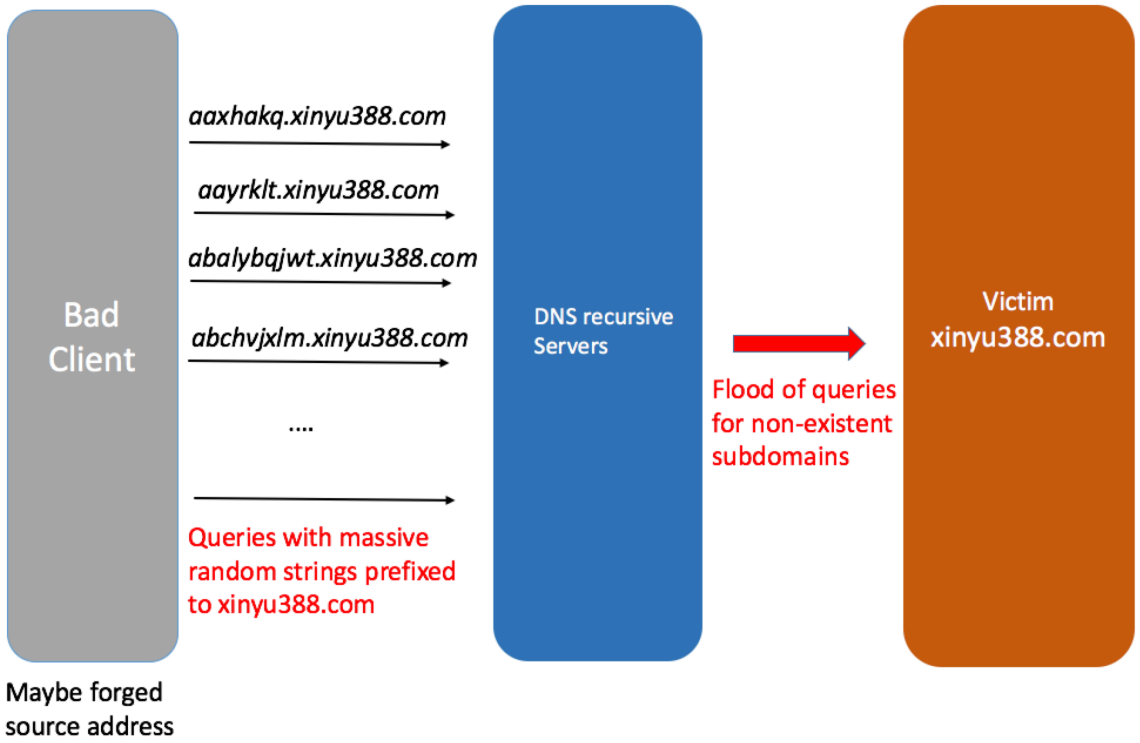
- 72207 DNS reflection/amplification attacks we see between 10.2 – 10.8

Realtime DNS Traffic – DNS Random subdomain attack

- Random subdomain attacks
  - High volume of queries for nonexistent subdomains
    - Nonexistent subdomains so no local cache
    - So the query will always reach the dns authoritative server
  - Mostly dns open resolvers as query sources
  - to attack DNS authoritative server

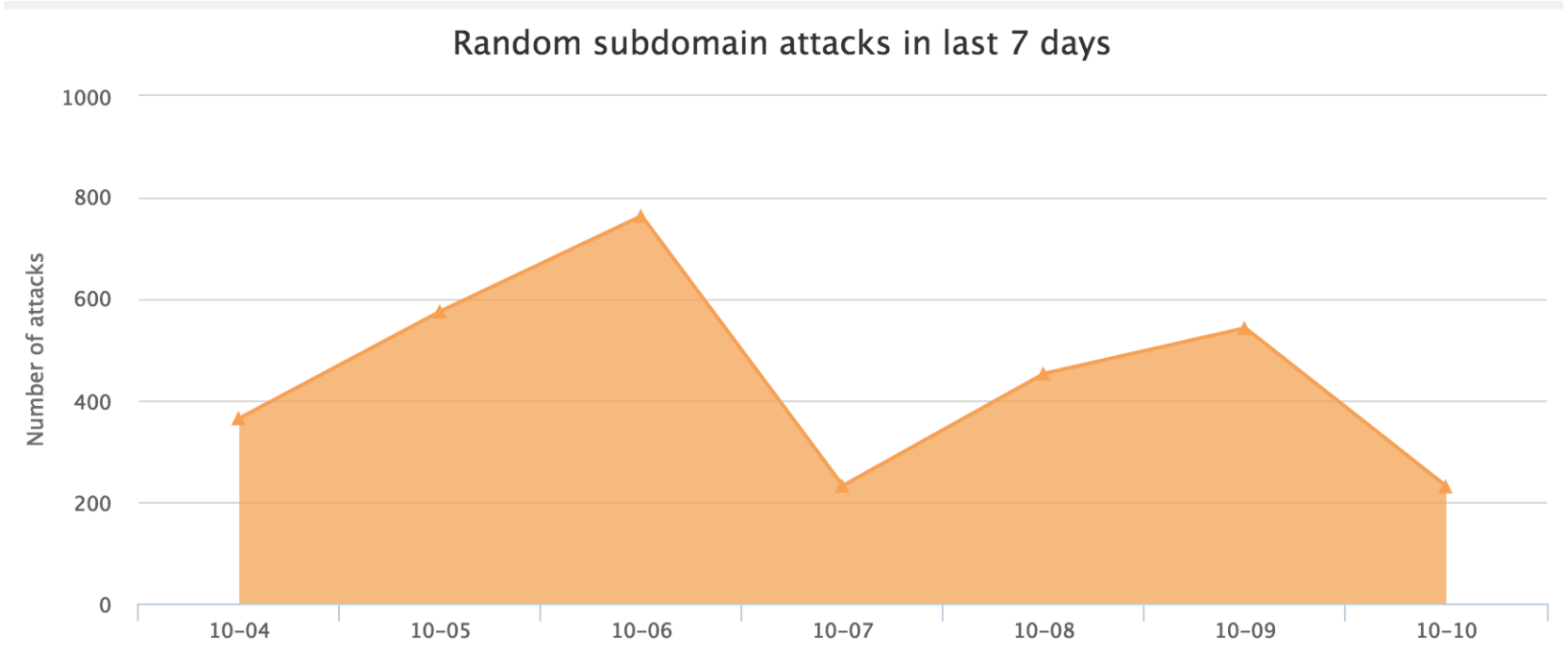
Realtime DNS Traffic – DNS Random subdomain attacks

- Example
  - xinyu388.com was attacked on 2016-10-09
  - 14809 random subdomain be detected



Realtime DNS Traffic – DNS Random subdomain attacks

- 3369 random subdomain attacks were detected in 7 days(Oct 4-10)



3: DDoS Botnet Command Tracking System

- A live DDoS botnet C2 tracking system
  - For some big ddos botnet families, track and analysis their C2 communication protocols
  - ~190k C2 servers (IP + Port)
  - Logged ~600M DDoS related instructions
  - ~40 common DDoS families are being tracked
    - Elknot/BillGates, XOR.DDoS, Mr.Black, Gafgyt, Nitol, etc

DDoS Botnet Tracking System

- Example
  - www.microsoft.com (**23.73.108.99**) was SYN flooded on 2016-09-23
  - 18 related C2(Command & Controller) servers captured in this attack
  - Mulite C2 instructions been logged

Botnet Command Tracked

Bot Family	C2 Server	C2 IP	C2 Port	Attack Type	Target Host	Target Port	Notes	Time
ldx	ppp.xxxatat456.com	149.202.219.49	1522	syn_flood	23.73.108.99	80	syn_flood, target=23.73.108.99...	2016-09-23 01:57:40
ldx	ppp.xxxatat456.com	149.202.219.49	1523	syn_flood	23.73.108.99	80	syn_flood, target=23.73.108.99...	2016-09-23 01:57:40
ldx	ppp.xxxatat456.com	149.202.219.49	1520	syn_flood	23.73.108.99	80	syn_flood, target=23.73.108.99...	2016-09-23 01:57:40
ldx	ppp.gggatat456.com	164.132.170.78	1520	syn_flood	23.73.108.99	80	syn_flood, target=23.73.108.99...	2016-09-23 01:57:43
ldx	ppp.gggatat456.com	164.132.170.78	1523	syn_flood	23.73.108.99	80	syn_flood, target=23.73.108.99...	2016-09-23 01:57:42
ldx	ppp.gggatat456.com	164.132.170.78	1522	syn_flood	23.73.108.99	80	syn_flood, target=23.73.108.99...	2016-09-23 01:57:42

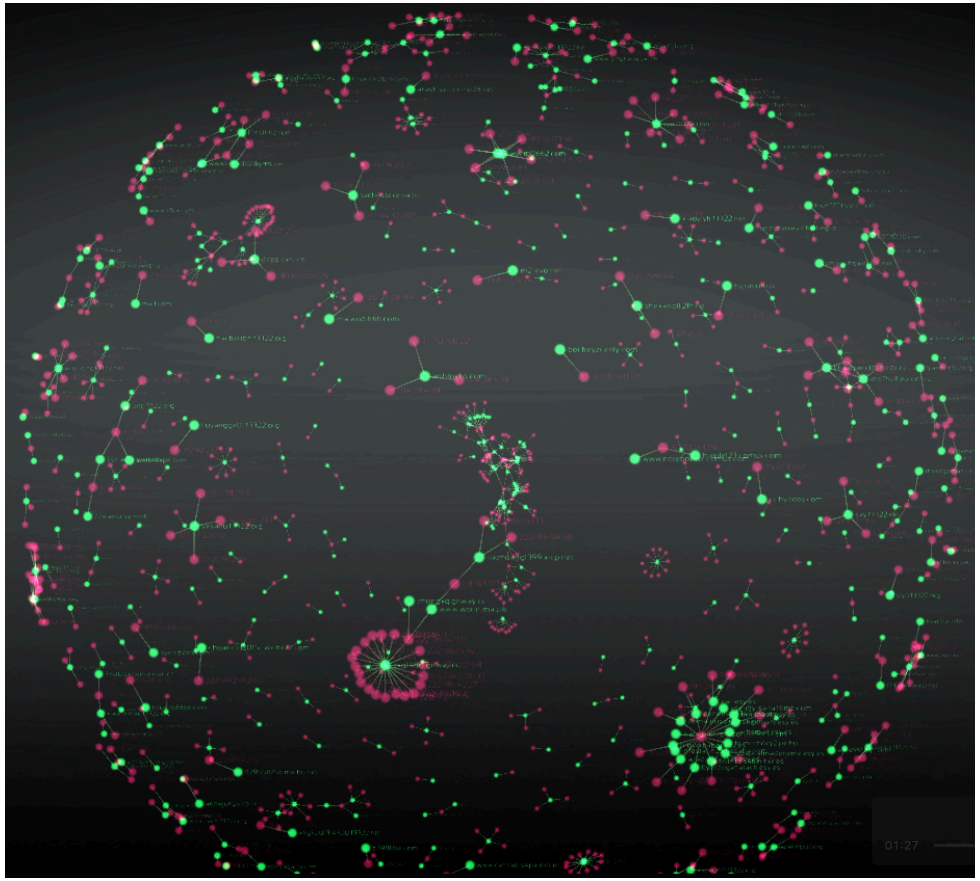
DDoS Botnet Tracking System

- Botnet command and controller(C2) and attacking instructions have been logged
  - time botname cc_server cc_ip cc_port type atk_type target_host target_port notes
  - 2016-09-23 01:57:43 ldx aaa.gggatat456.com 164.132.170.78 6003 ddos syn_flood 23.73.108.99 80 syn_flood, target=23.73.108.99, port=80, atk_time=30s, payload_size=888, tasks=11, use_fake_source_ip

  - C2 family: LDX
  - C2 server: *aaa.gggatat456.com* (164.132.170.78)
  - C2 Port: 6003
  - Attack: syn flood
  - Target ip and port 23.73.108.99(Microsoft) port 80

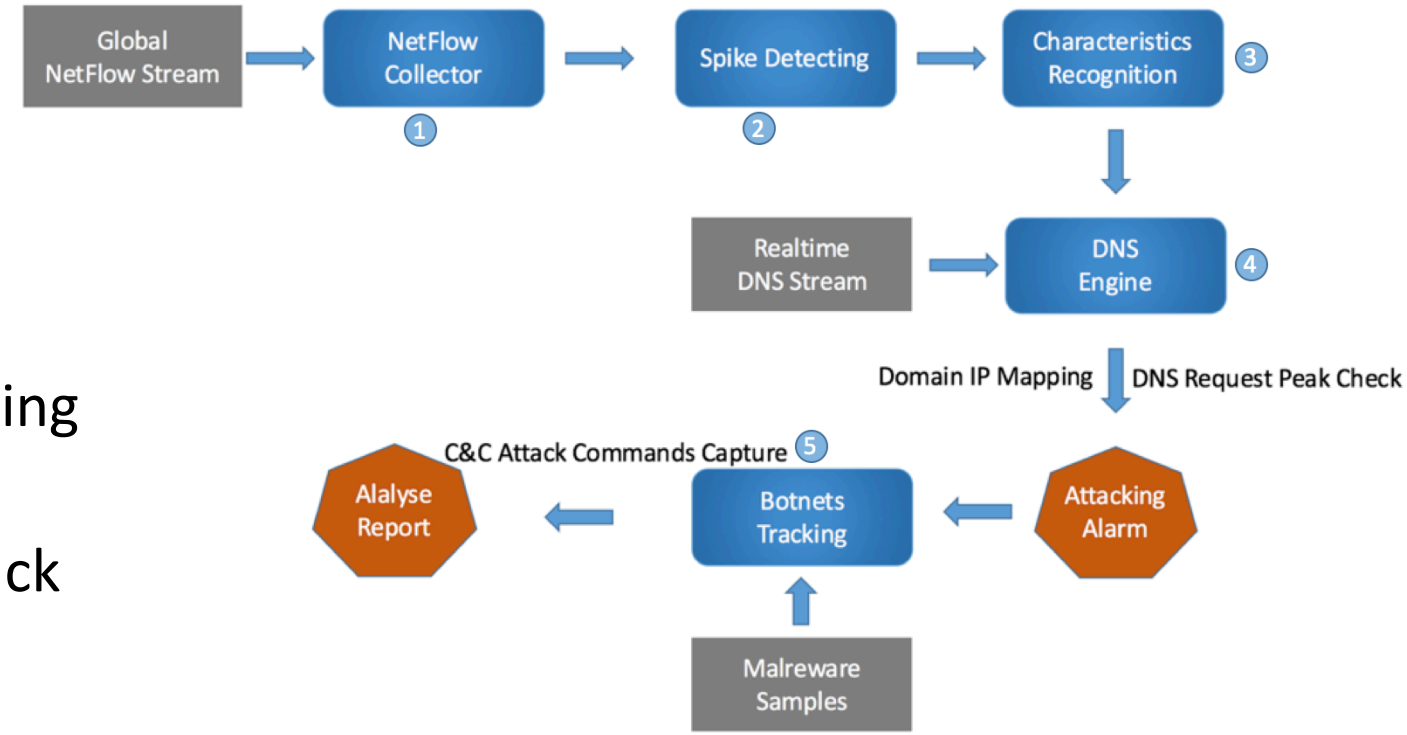
DDoS Botnet Tracking System

- A video clip to show some major C2s and their IPs, you will see some big C2 clusters and some of the C2 form some sort of relations



Recap: How DDoSMon Detecting DDoS ?

- Realtime NetFlow traffic
  - Spike Detecting
  - Characteristics recognition
- Realtime DNS traffic
  - Domain diemension monitoring
  - DNS reflection attack
  - DNS random subdomain attack
- DDoS botnet C2 tracking



Use DDoSMon

- Just apply a free account
- Create monitored objects(IP, Net blocks, FQDN or DNS zones) you are interested
- Then system will take care of the rest automatically

- If attack happen, you will receive an email notification
- Elaborate report, get insights about the attack

How can I contribute

- More netflow data means more coverage
  - Have netflow data to contribute?
- Submit DDoS related malware samples

Thanks, Q&A

gongyiming@360.cn
keqiang@360.cn
netlab.360.com