scanning

Matsuzaki ‘maz’ Yoshinobu

<maz@iij.ad.jp>

nmap (https://nmap.org)

- Nmap is a free and open source network utility for network discovery and security auditing
- Working on all major OSes
- It uses raw IP packets to determine
  - what hosts are available on the network
  - what services those hosts are offering
  - what operating systems they are running
  - what type of packet filters/firewalls are in use

Ethical Issue

- Unauthorized use of Nmap on a system could be illegal depending on regulations
- Make sure you get a proper permission from the target owner before using this tool
- There is no right way to do the wrong things

Nmap : How it works

- DNS lookup-matches name with IP
- Nmap pings the remote target with 0 (zero) byte packets to each port
- If packets are not received back, port is open
- If packets are received, port is closed
- Firewall can interfere with this process

Nmap : Scanning Techniques

- Host Discovery and Target Specification
- Port Scanning Technique, Specification and order
- OS, Service and Version Detection
- namp Scripting Engine
- Timing and Performance
- Firewall, IDS Evasion and Spoofing Technique
- Scan Report

Nmap: Scan

```
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
```

OS DETECTION:

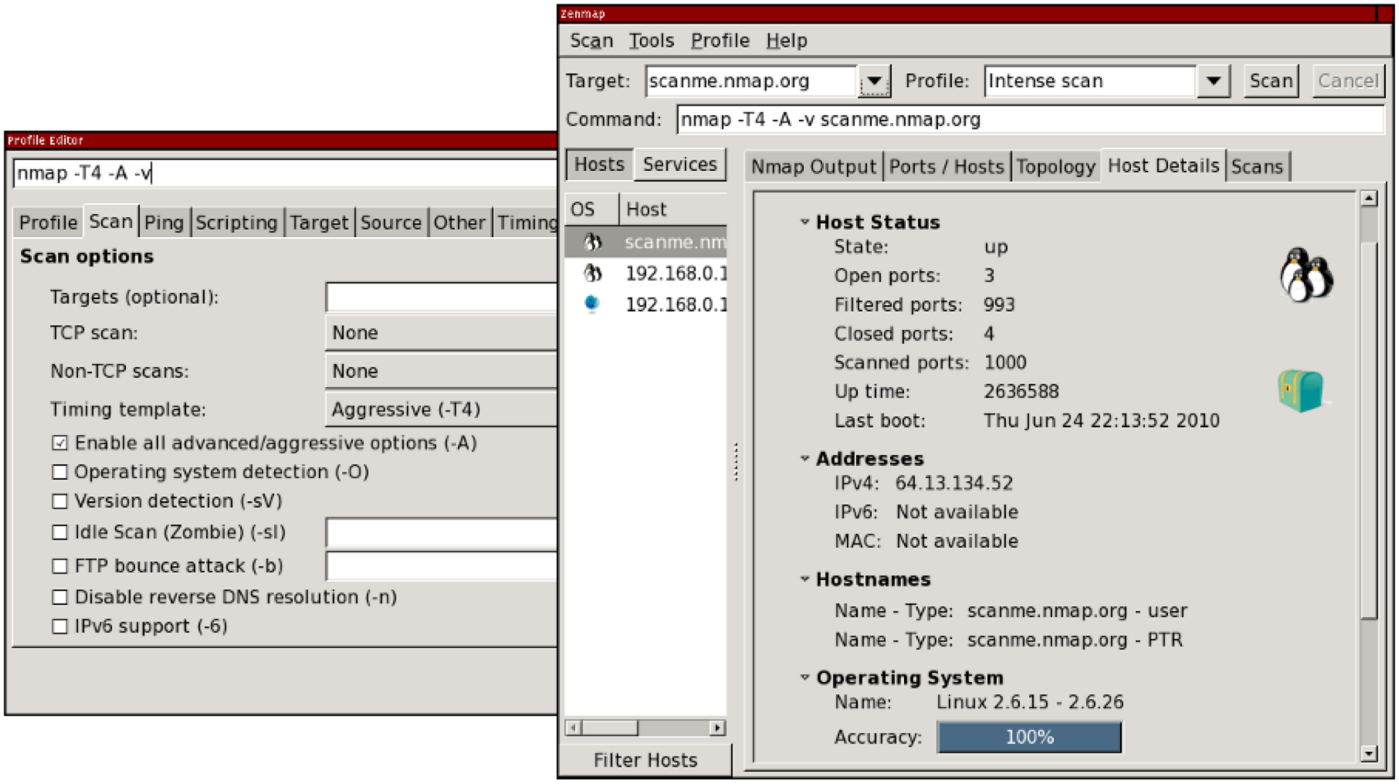
-O: Enable OS detection

--osscan-limit: Limit OS detection to promising targets

--osscan-guess: Guess OS more aggressively

```
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
```

Zenmap(GUI) for Windows

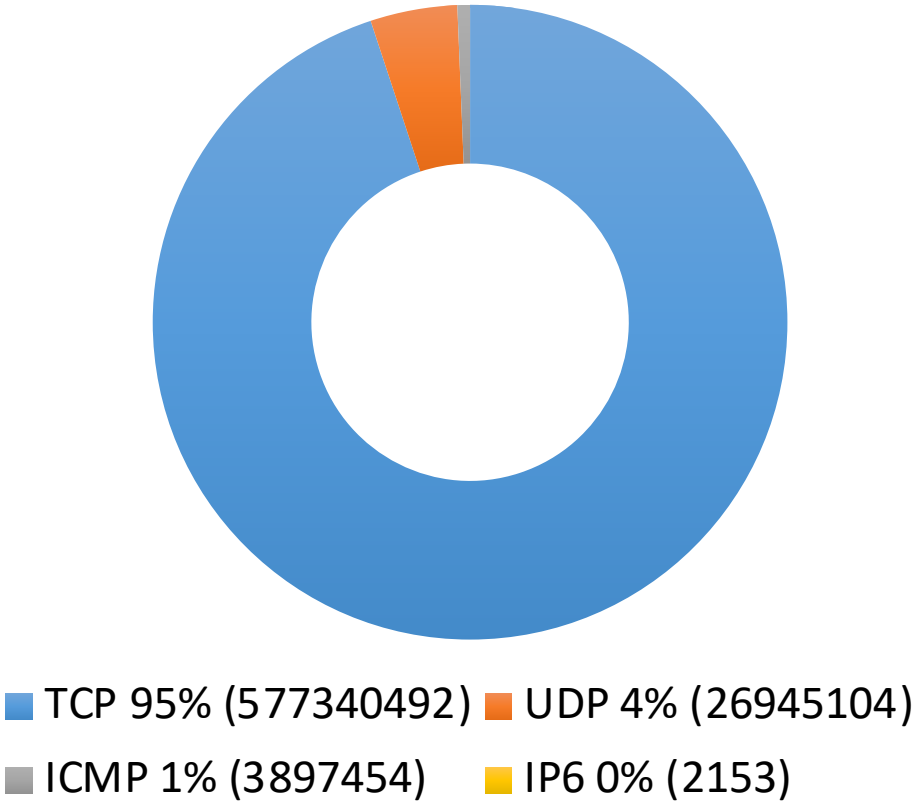


https://nmap.org/book/zenmap.html

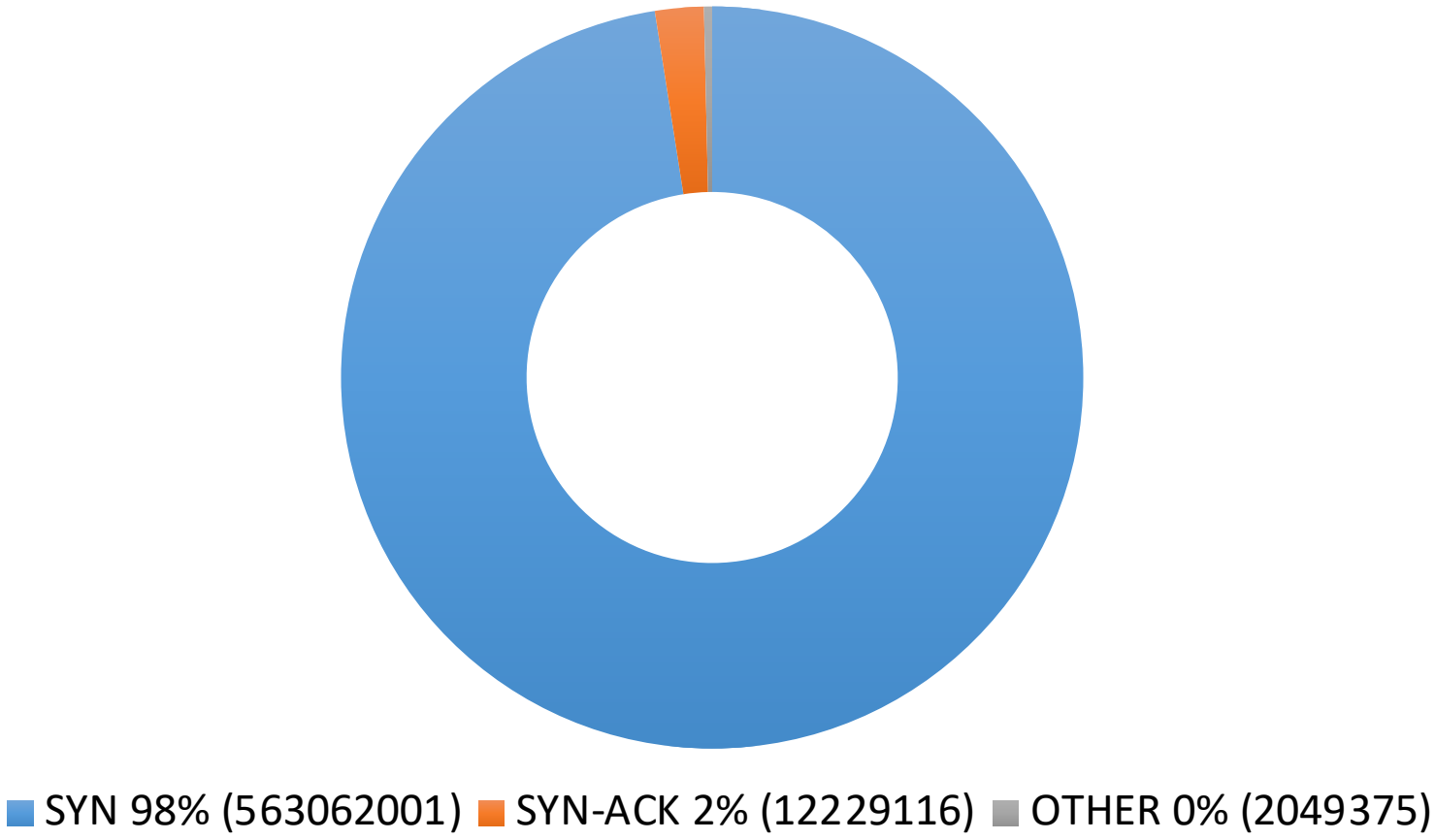
Some study based on PPP-EXP

- Duration: 2019/01/10 00:00~24:00(JST)
- Fully captured incoming packets toward the prefixes
  - https://www.attn.jp/ppp/
  - 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

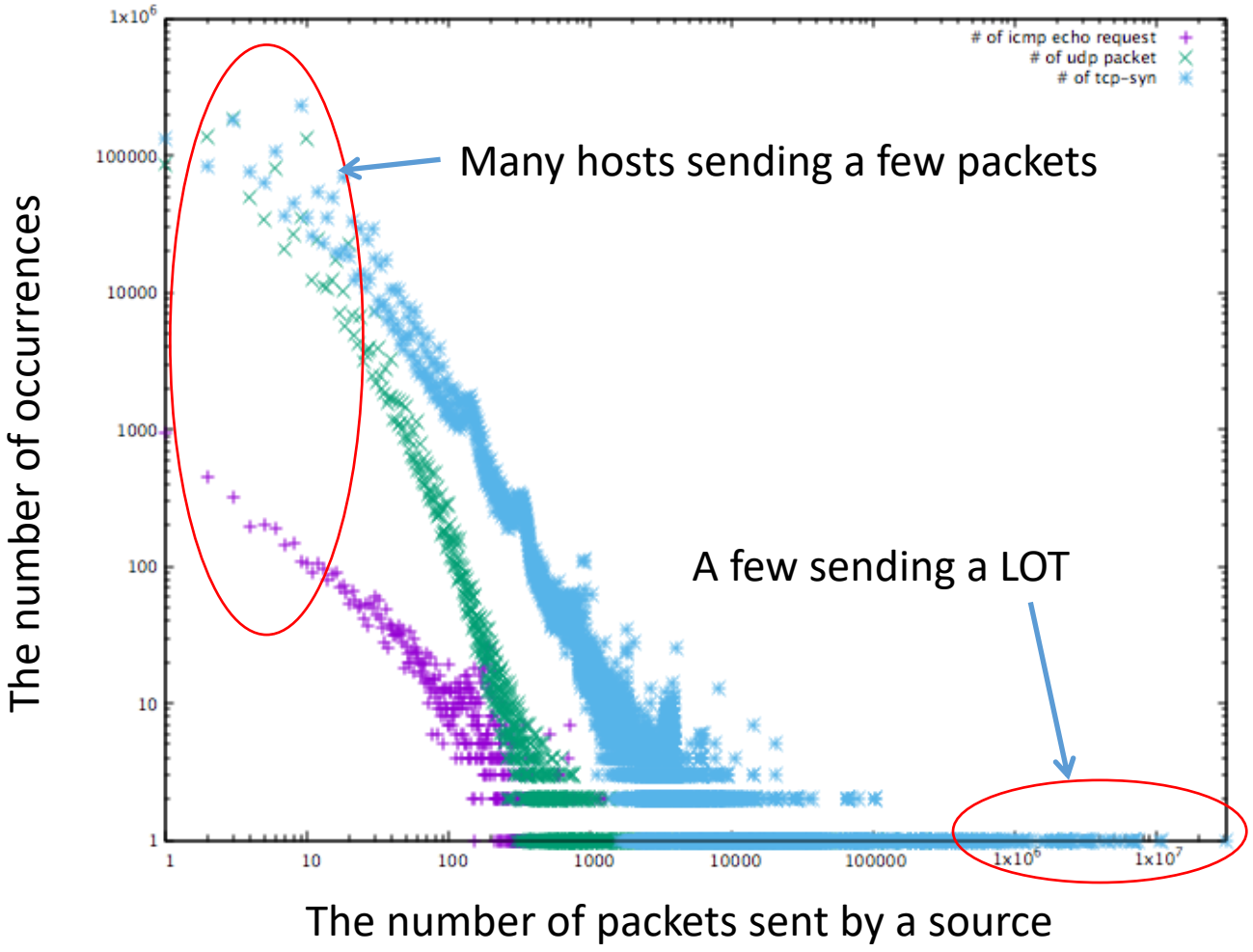
TCP-SYN destinations

• 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

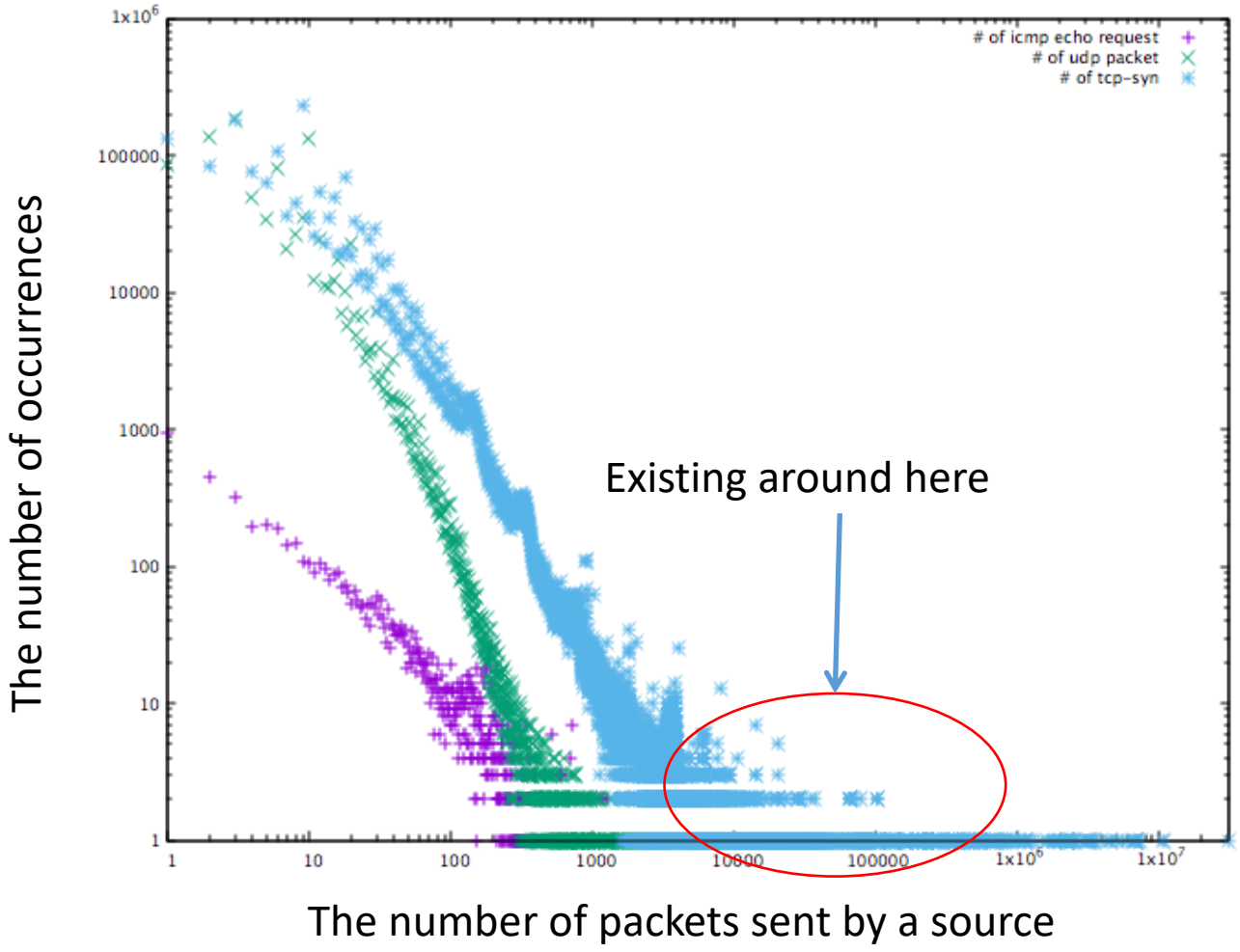
Packets distribution: Sender



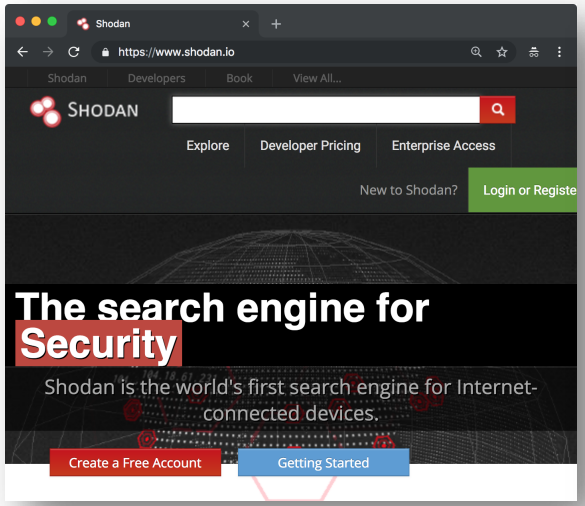
A few hosts sending a lot of packets

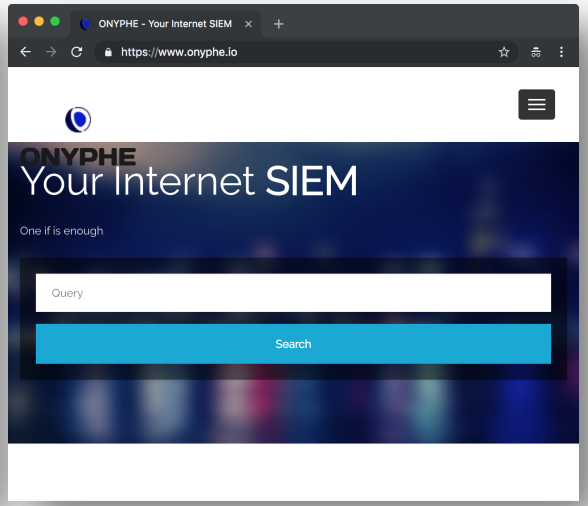
- Ukrainian IP (31609992 packets)
  - TCP-SYN to TCP/1025-10000
- USA IP (10793632 packets)
  - TCP-SYN to TCP/52869
- Dutch IP (10572421 packets)
  - TCP-SYN to TCP/52869
- HongKong IP (7330971 packets)
  - TCP-SYN to TCP/3031 and other 546 ports
- Ireland 8 IPs (total 51607564packets)
  - TCP-SYN to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

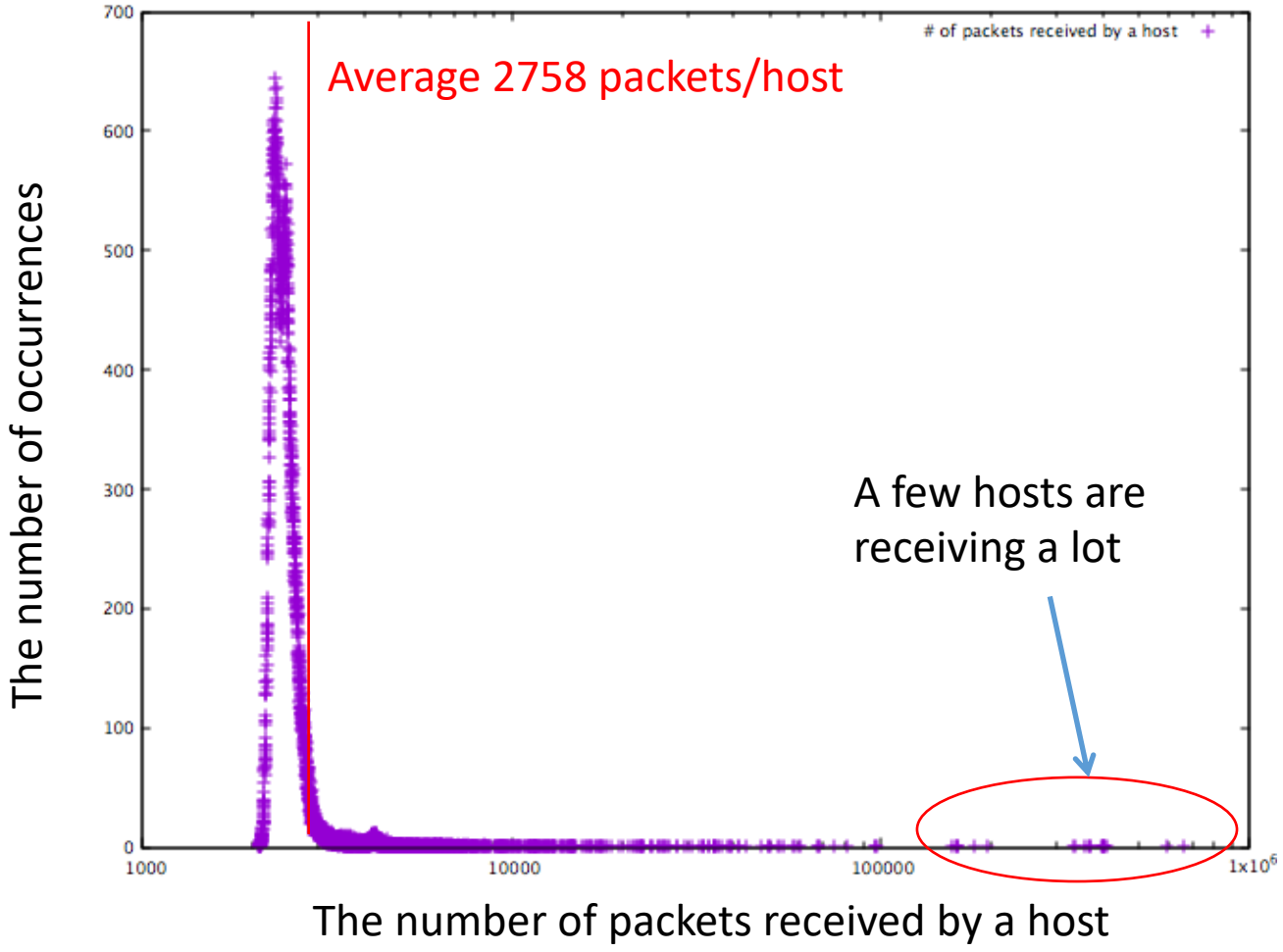
```
02:23:47.578188 IP 171.36.43.8.30834 > 219.101.115.202.766: UDP, length 482
        0x0000:  4500 01fe 6b0f 4000 3311 b583 ab24 2b08  E...k.@.3....$+.
        0x0010:  db65 73ca 7872 02fe 01ea 221b 6e8e b267  .es.xr....".n..g
        0x0020:  efe6 db0d d926 9c87 28c9 64a4 94e6 f1cf  .....&..(.d.....
        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?

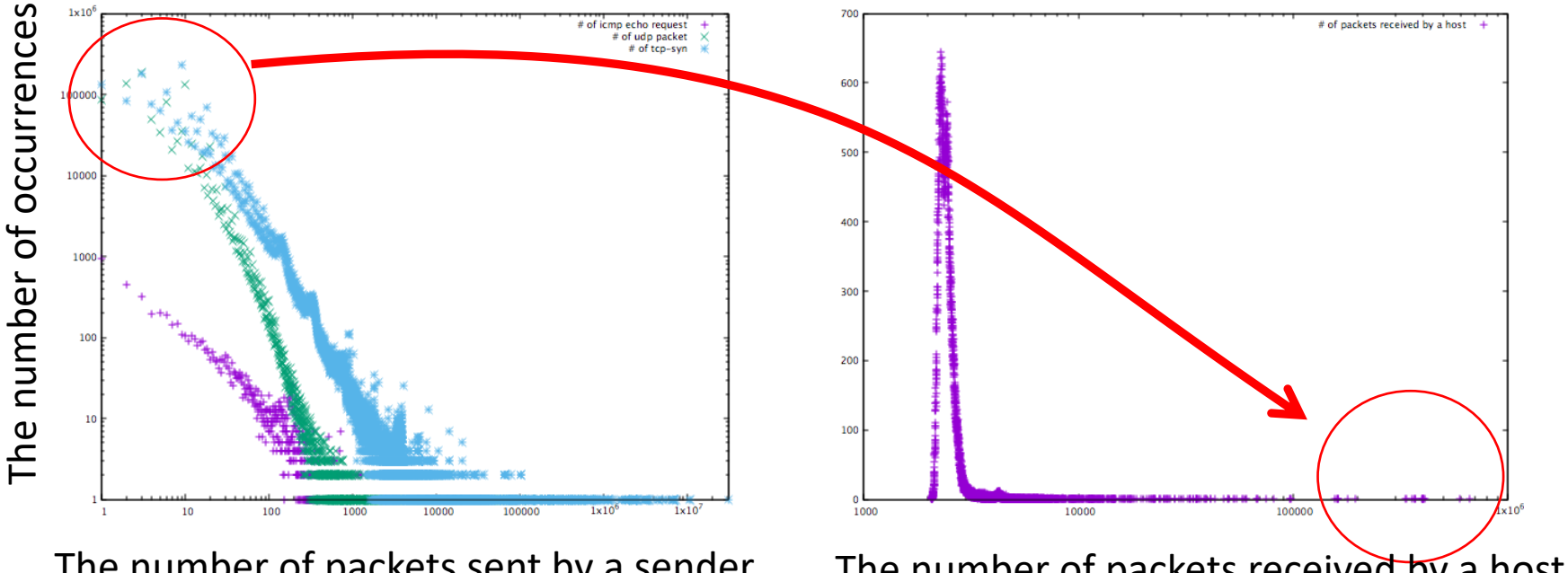
- The number of unique senders might be indicating the number of P2P users

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