Zeroing in on Port 0 Traffic in the Wild

Aniss Maghsoudlou

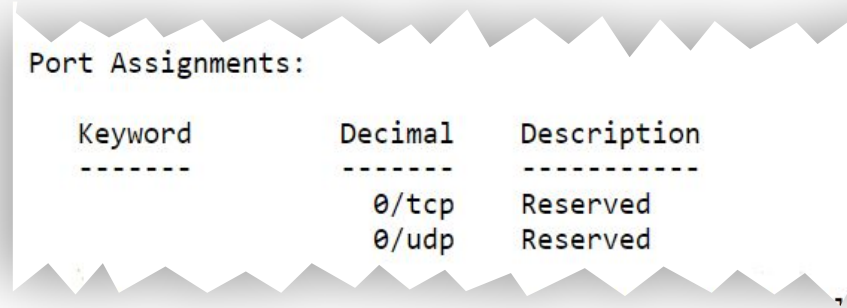
Oliver Gasser

Anja Feldmann

Max Planck Institute for Informatics

Why Port 0?

RFC1340: Port 0 is reserved for UDP and TCP.



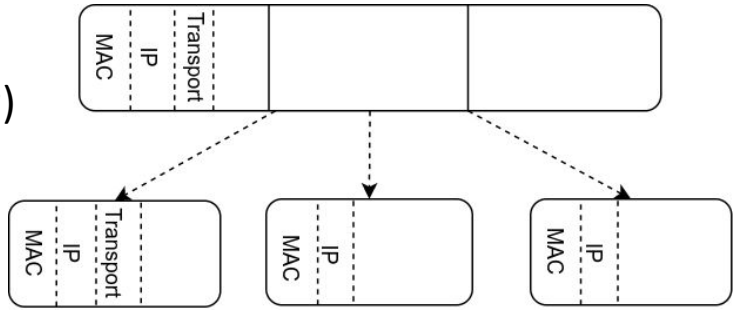
```
Port Assignments:

   Keyword          Decimal    Description
   -------          -------    -----------
                      0/tcp    Reserved
                      0/udp    Reserved
```

720 TB of traffic using port 0 in one week of IXP data!

IXP

- A significant number of packets
  - Have srcport = 0 & dstport = 0 (UDP&TCP)
  - Contain payload
  - Set TCP flags to 0



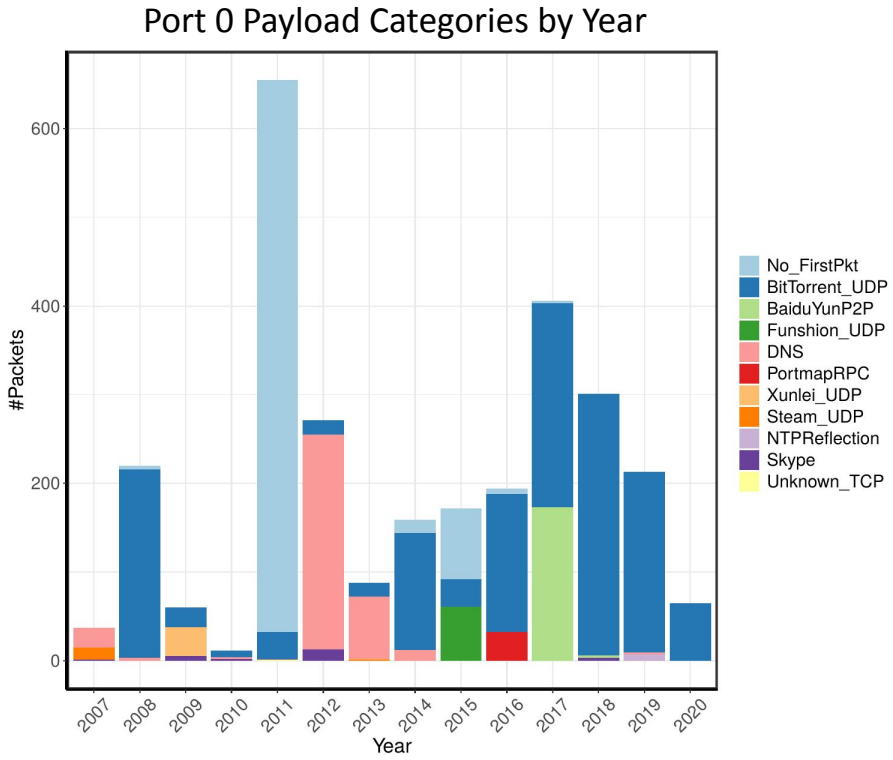
- IXP operators confirmed:
  - Flow exporters zero out missing UDP/TCP headers in non-initial fragments

➠ Packet fragmentation is possibly responsible.

MAWI

- Applications using port 0 change over time.
- **BitTorrent** is a constant contributor to port 0 traffic in different years.

BitTorrent

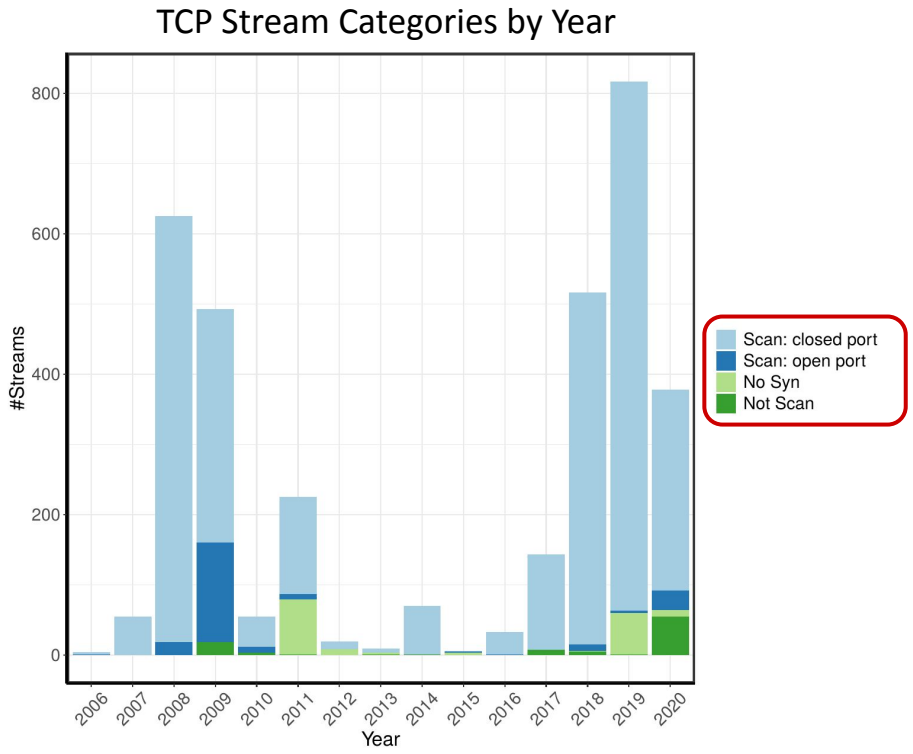


max planck institut informatik

MAWI

- A large fraction of the TCP streams are **one-way**.
- A major fraction of **two-way** TCP streams are scans to closed ports.

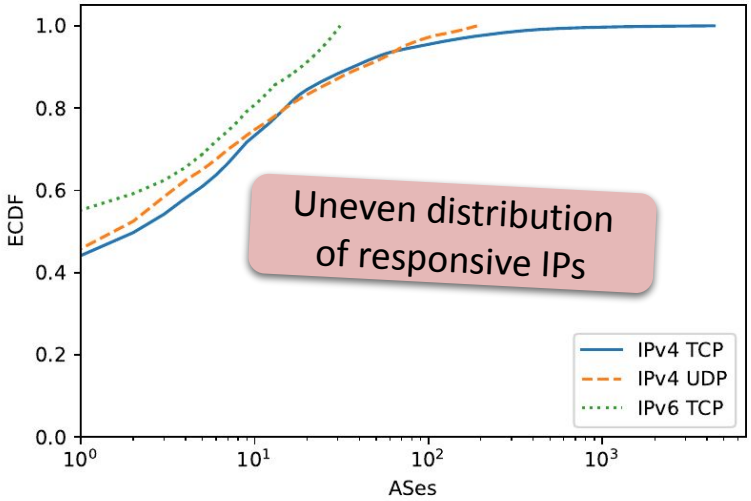
Scanning



Active Measurement

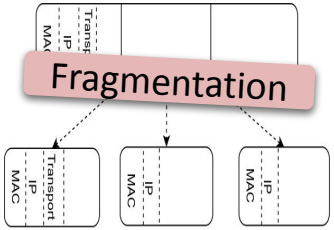
Q: Can we confirm that there are hosts with open port 0 in the wild?

- Analyze responsiveness of IP addresses to port 0 probes (ZMap)
  - No responsive address to IPv6 UDP probes
  - More responses in TCP compared to UDP
  - Of all responses for IPv4 TCP, IPv4 UDP, and IPv6 TCP:
    - > 40% come from only one AS
    - > 70% come from 10 ASes



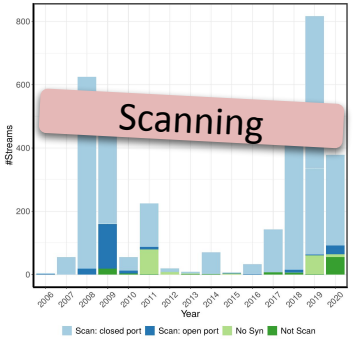
max planck institut informatik

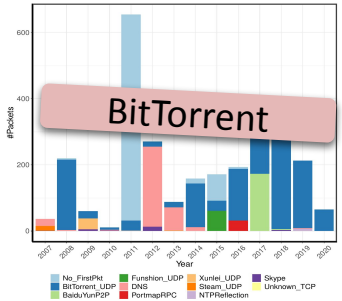
Conclusion



Port 0 Service:

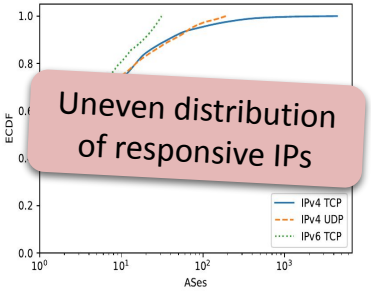
https://inet-port0.mpi-inf.mpg.de/





Aniss Maghsoudlou

aniss@mpi-inf.mpg.de



max planck institut informatik