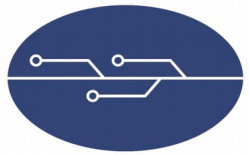
Network Telescopes Revisited

From Loads of Unwanted Traffic to Threat Intelligence

Piotr Bazydło, Adrian Korczak, Paweł Pawliński

Research and Academic Computer Network
(NASK, Poland)



SISSDEN

NASK

Who are we

Piotr Bazydło
Head of Network Security Methods Team NASK
@chudyPB
piotr.bazydlo@nask.pl

Adrian Korczak
Network Security Methods Team NASK
adrian.korczak@nask.pl

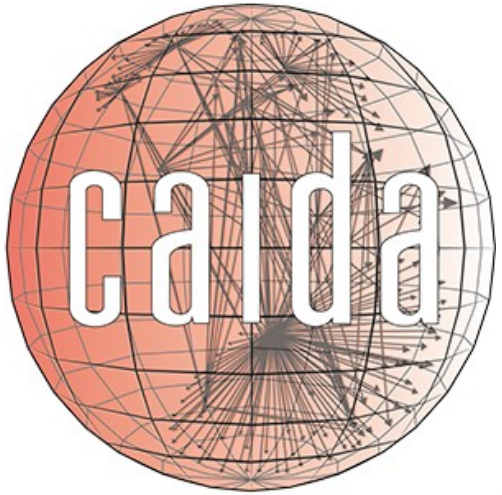
Paweł Pawliński
CERT Polska
pawel.pawlinski@cert.pl

NASK

Network Telescope

- Also known as **darknet** or blackhole.
- Unused IP address space.
- No legitimate network traffic should be observed.

- First (?) & largest telescope (approx /8):



NASK

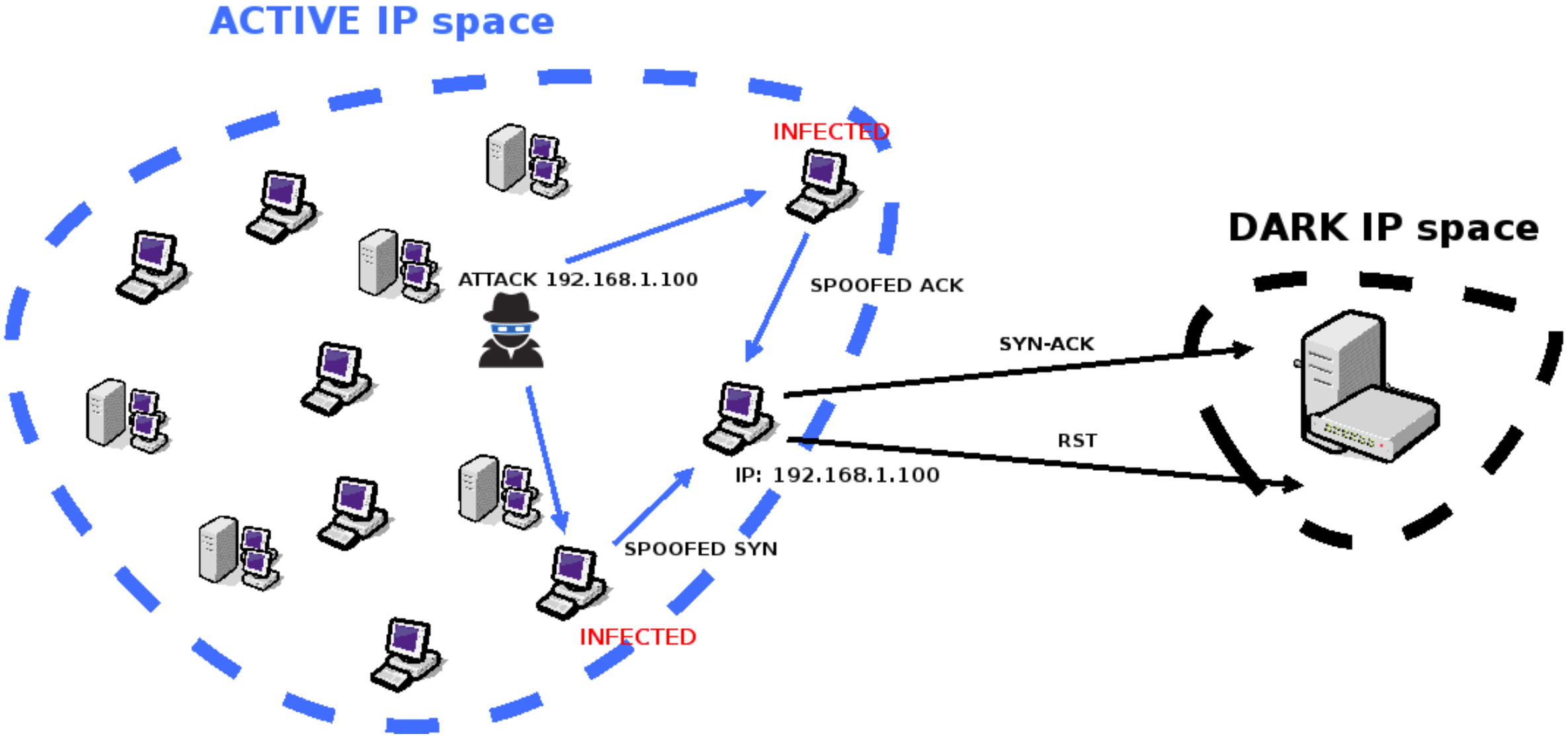
Network Telescope

In practice, we can see a lot of different activities:

- Misconfiguration of network devices/applications.
- Scanning.
- Backscatter from DoS attacks.
- Exploitation attempts (UDP).
- Weird stuff.

NASK

DoS attacks (backscatter)



NASK

What we want to achieve?

- Detect large-scale malicious events (botnets, exploits).
- Detect attacks on interesting targets.
- Track activities of specific actors responsible.
- Understand the dynamics (trends).

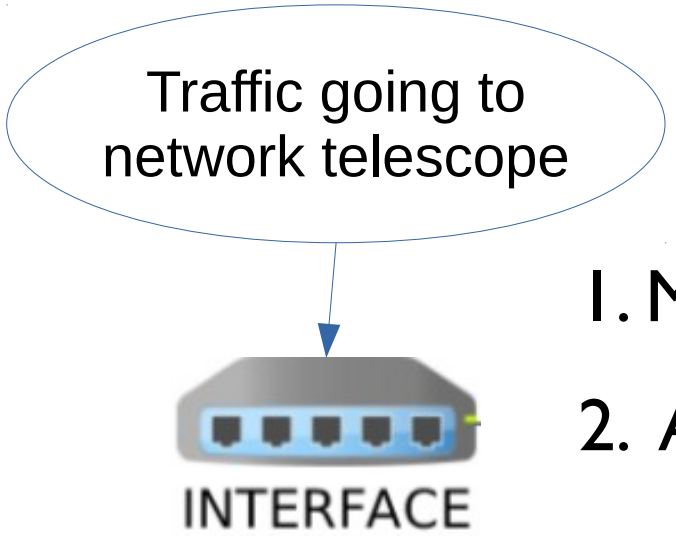
NASK

Problems

- How to group packets?
- How to classify them into events?
- How to find interesting events?
- How to identify actors?
- How to analyze trends?

NASK

Our approach



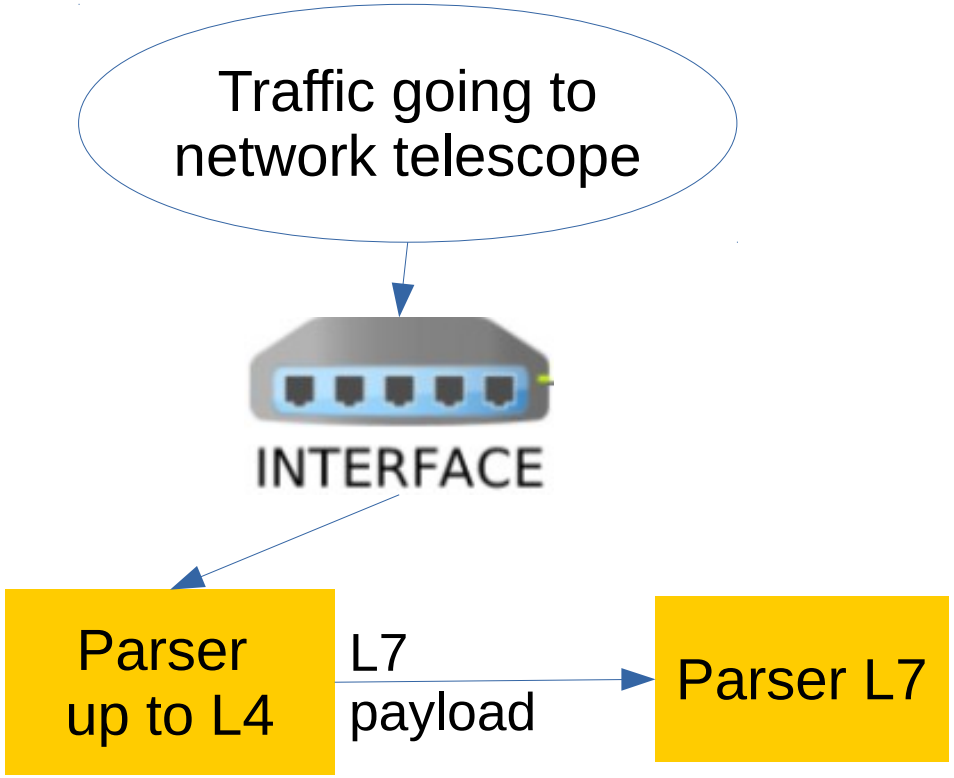
1. Monitored IPv4 space: **> 100 000** addresses
2. Analyze captured traffic every 5 minutes.

Stats:

~ 10 000 pps

~ 25 000 000 000 packets per month

80% = TCP



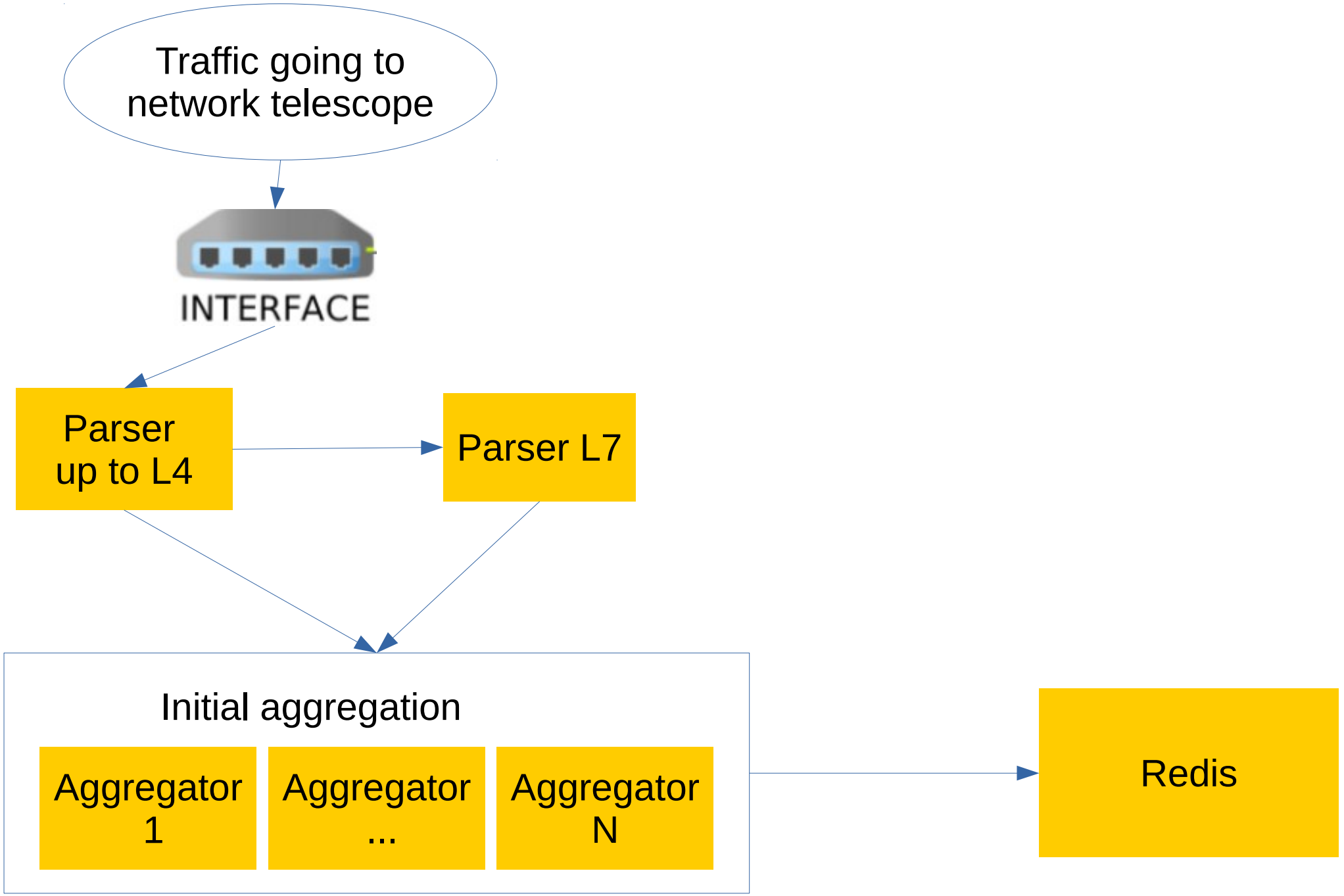
Two parsing scripts:

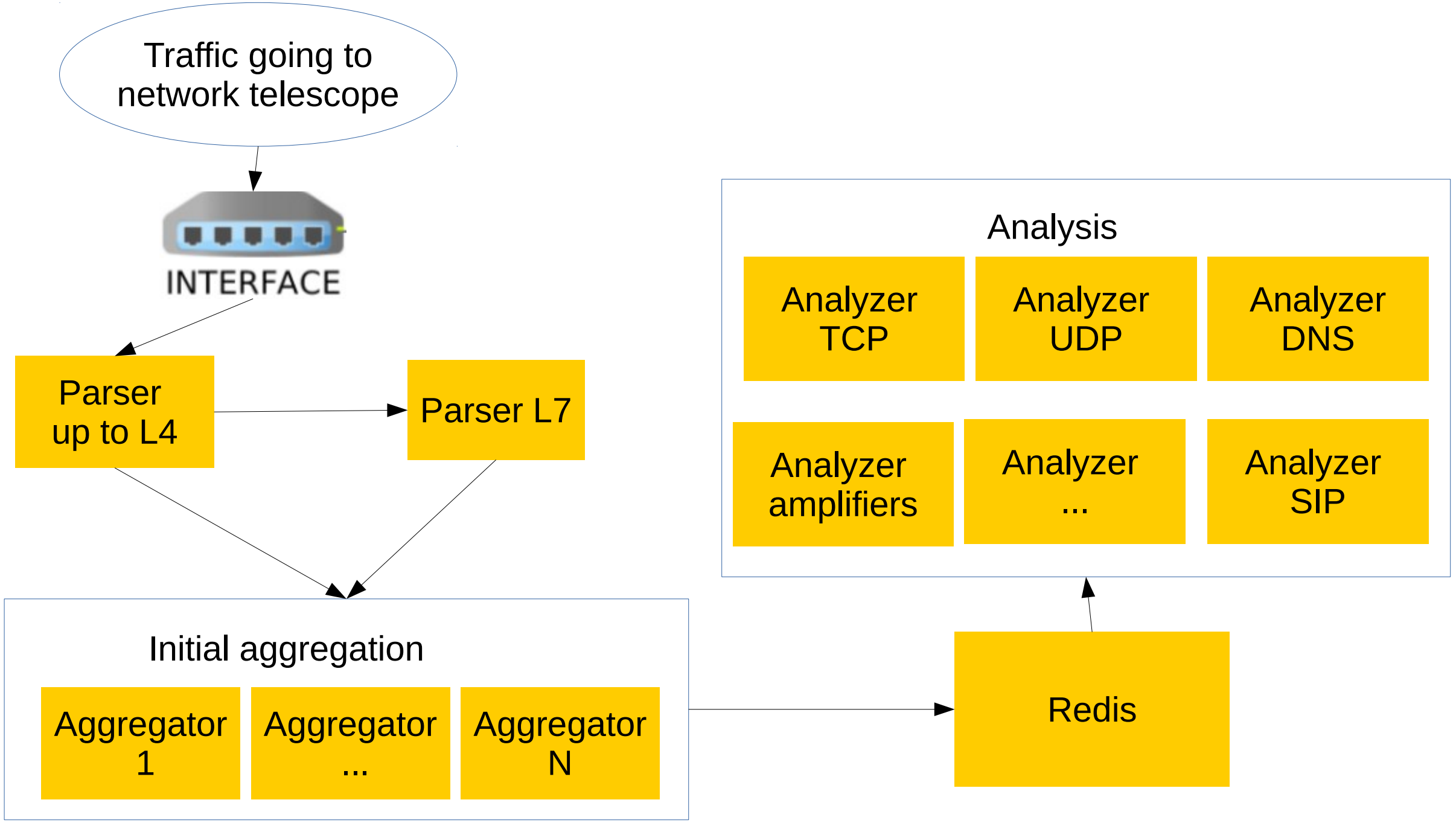
- Parser L4 – up to 4th OSI layer.

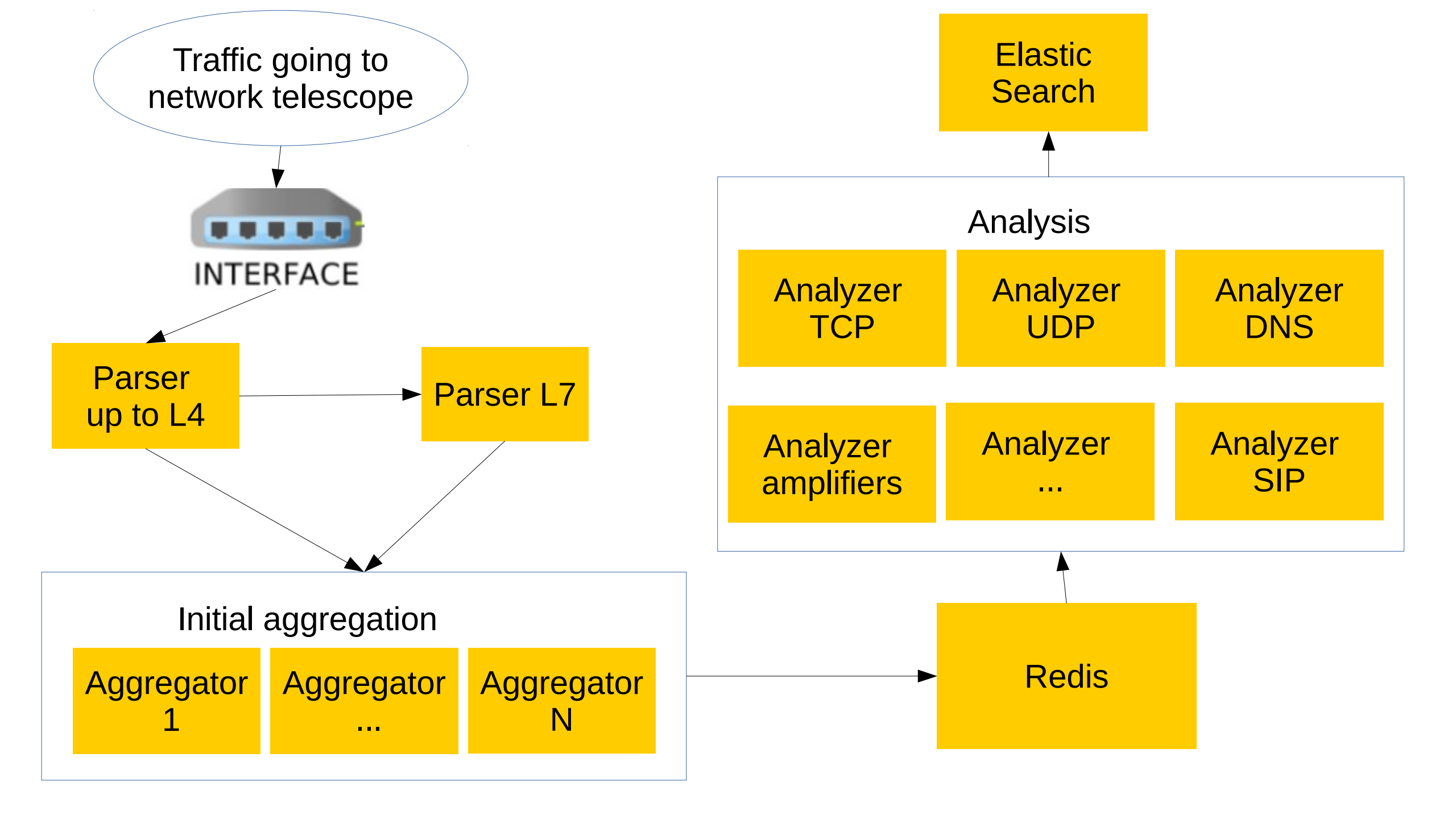
written in C++, uses libtins library.

- Parser 7 – parsing of 7th OSI layer.

written in python, uses dpkt library

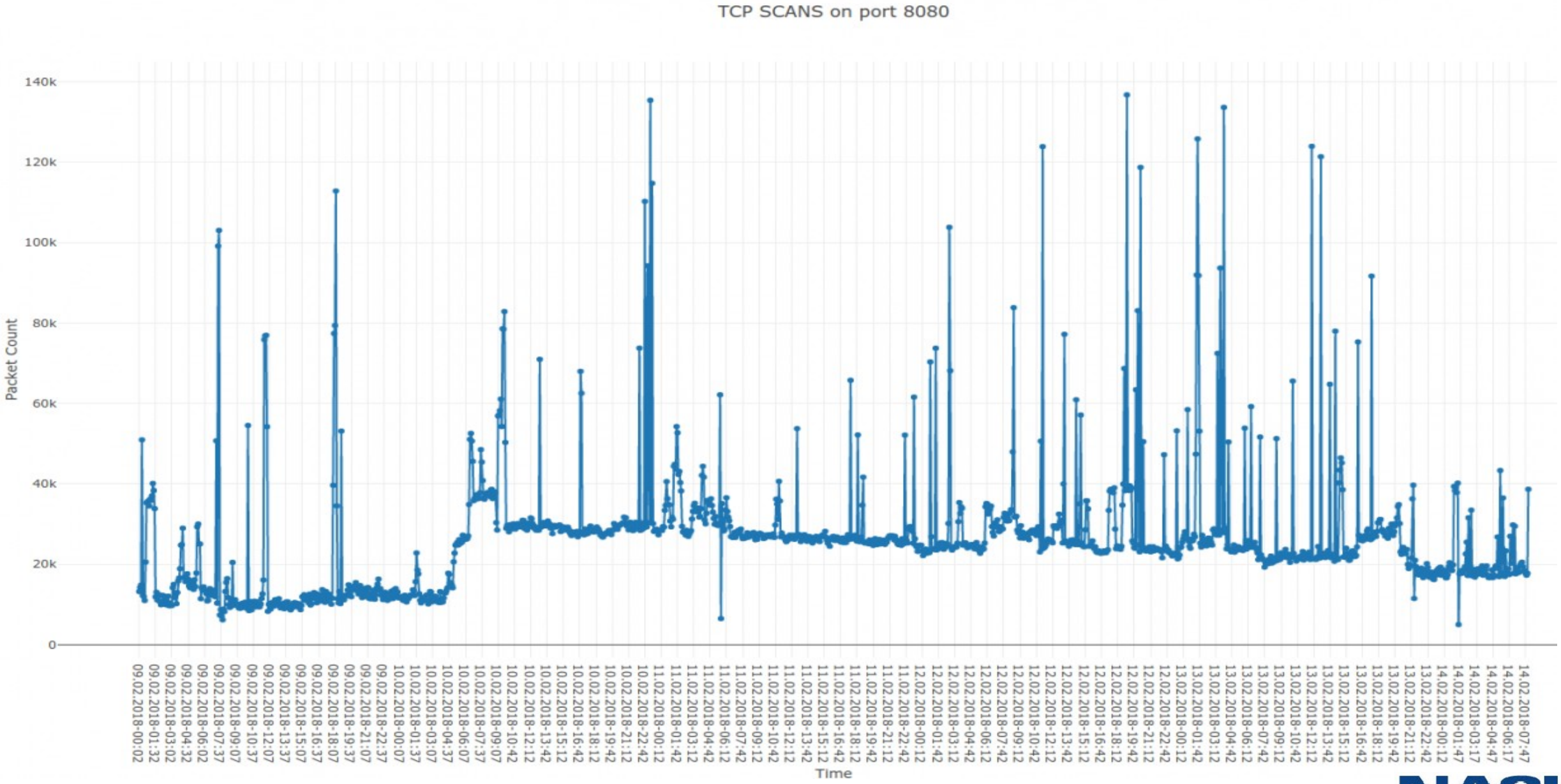

Traffic going to network telescope
INTERFACE
Parser up to L4
Parser L7
Initial aggregation
Aggregator 1
Aggregator ...
Aggregator N
Redis


Traffic going to network telescope
INTERFACE
Parser up to L4
Parser L7
Initial aggregation
Aggregator 1
Aggregator ...
Aggregator N
Redis
Analysis
Analyzer TCP
Analyzer UDP
Analyzer DNS
Analyzer amplifiers
Analyzer ...
Analyzer SIP

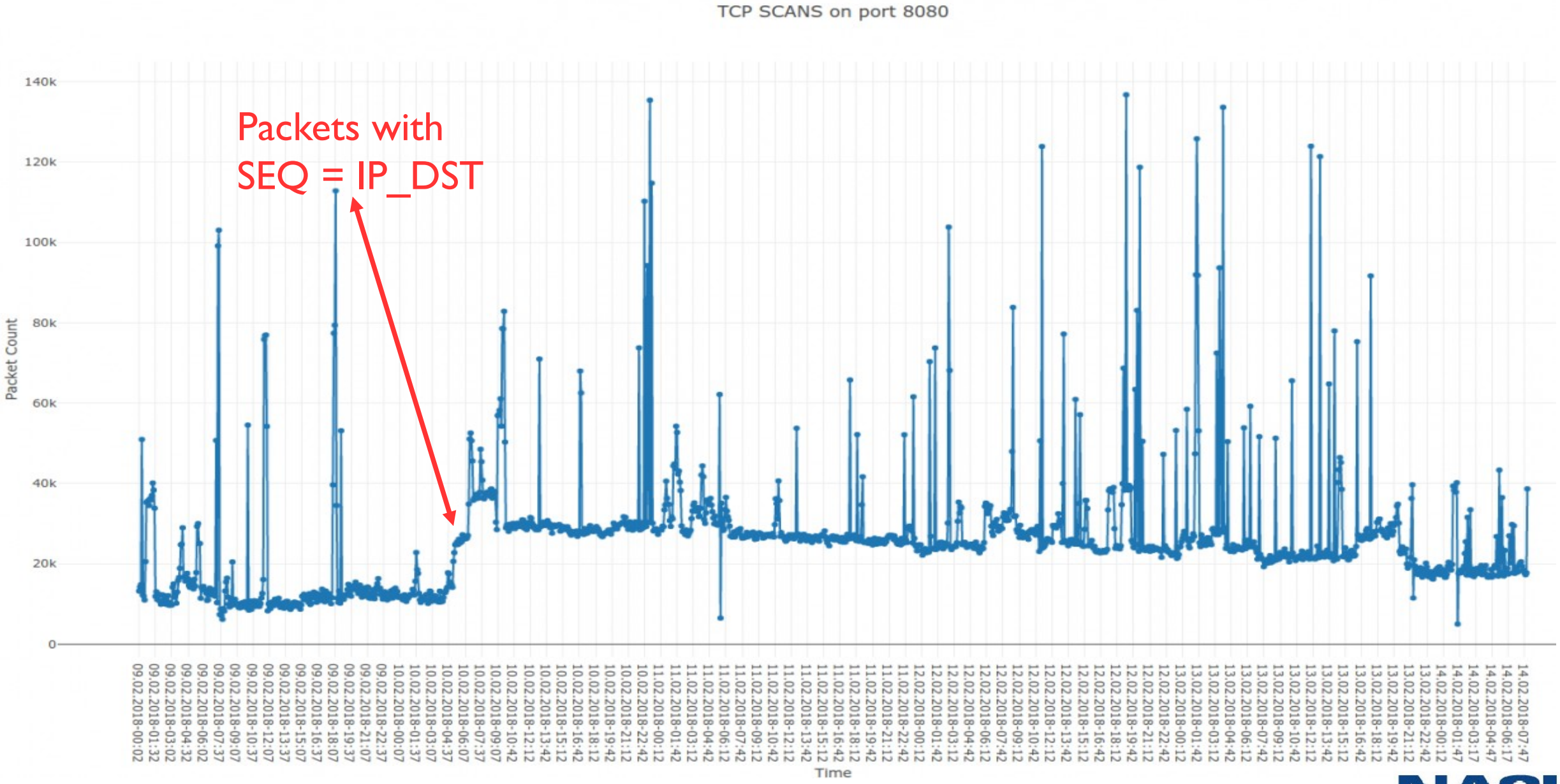

Traffic going to network telescope
INTERFACE
Parser up to L4
Parser L7
Initial aggregation
Aggregator 1
Aggregator ...
Aggregator N
Redis
Analysis
Analyzer TCP
Analyzer UDP
Analyzer DNS
Analyzer amplifiers
Analyzer ...
Analyzer SIP
Elastic Search

Case study 1
Botnet Fingerprinting

Botnet fingerprinting

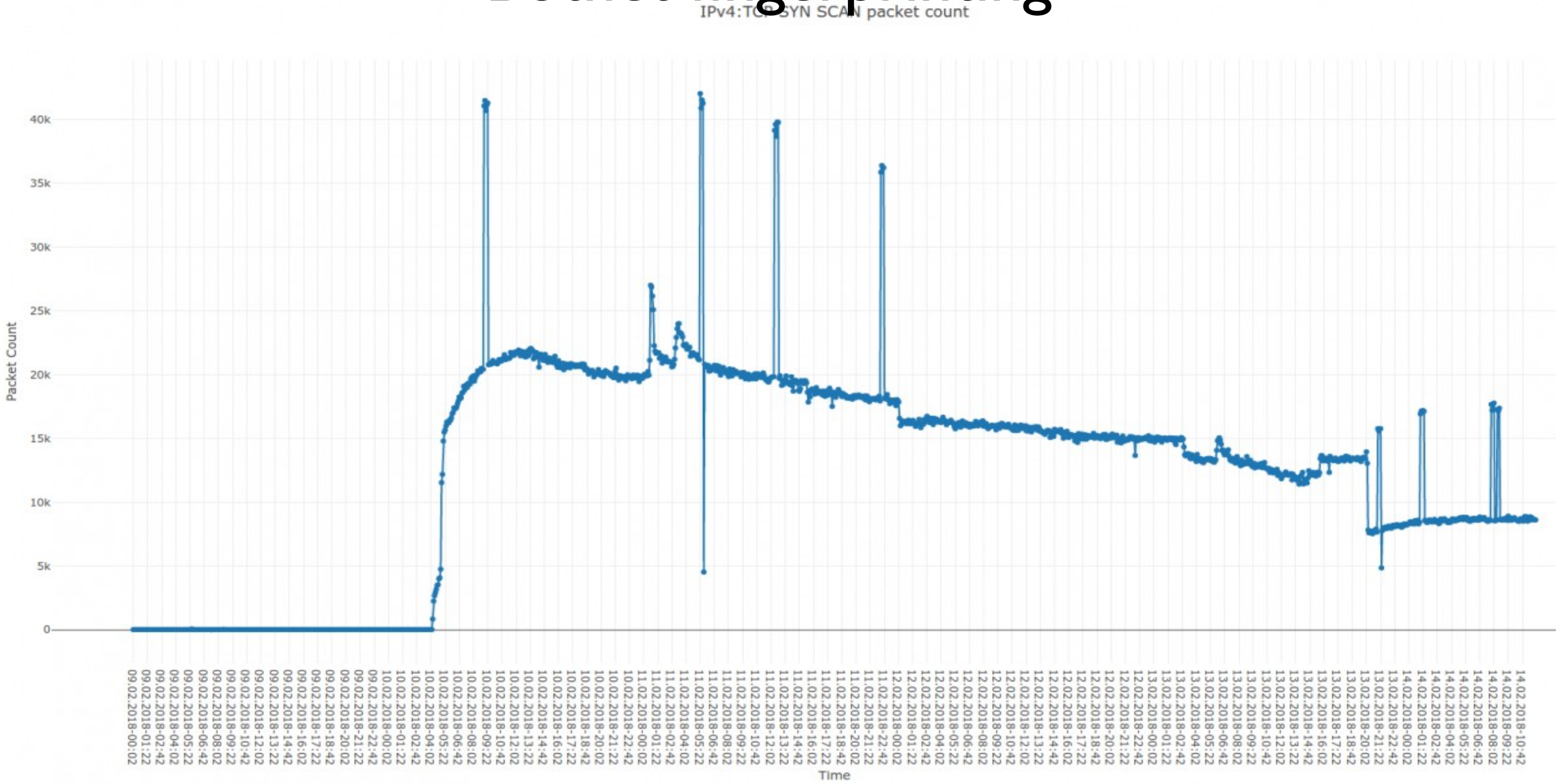


Botnet fingerprinting



NASK

Botnet fingerprinting



NASK

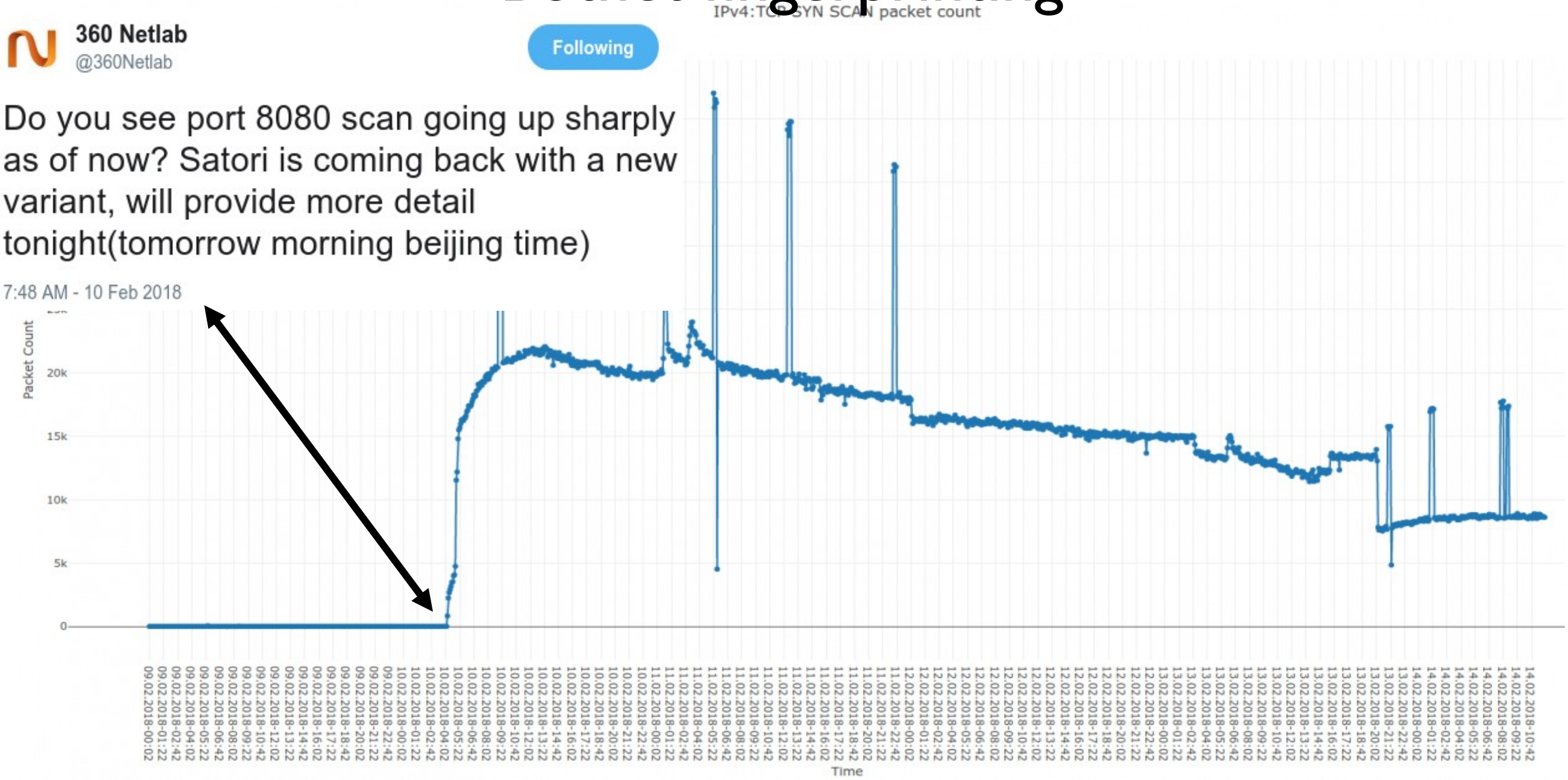
Botnet fingerprinting

360 Netlab
@360Netlab

Following

Do you see port 8080 scan going up sharply as of now? Satori is coming back with a new variant, will provide more detail tonight(tomorrow morning beijing time)

7:48 AM - 10 Feb 2018

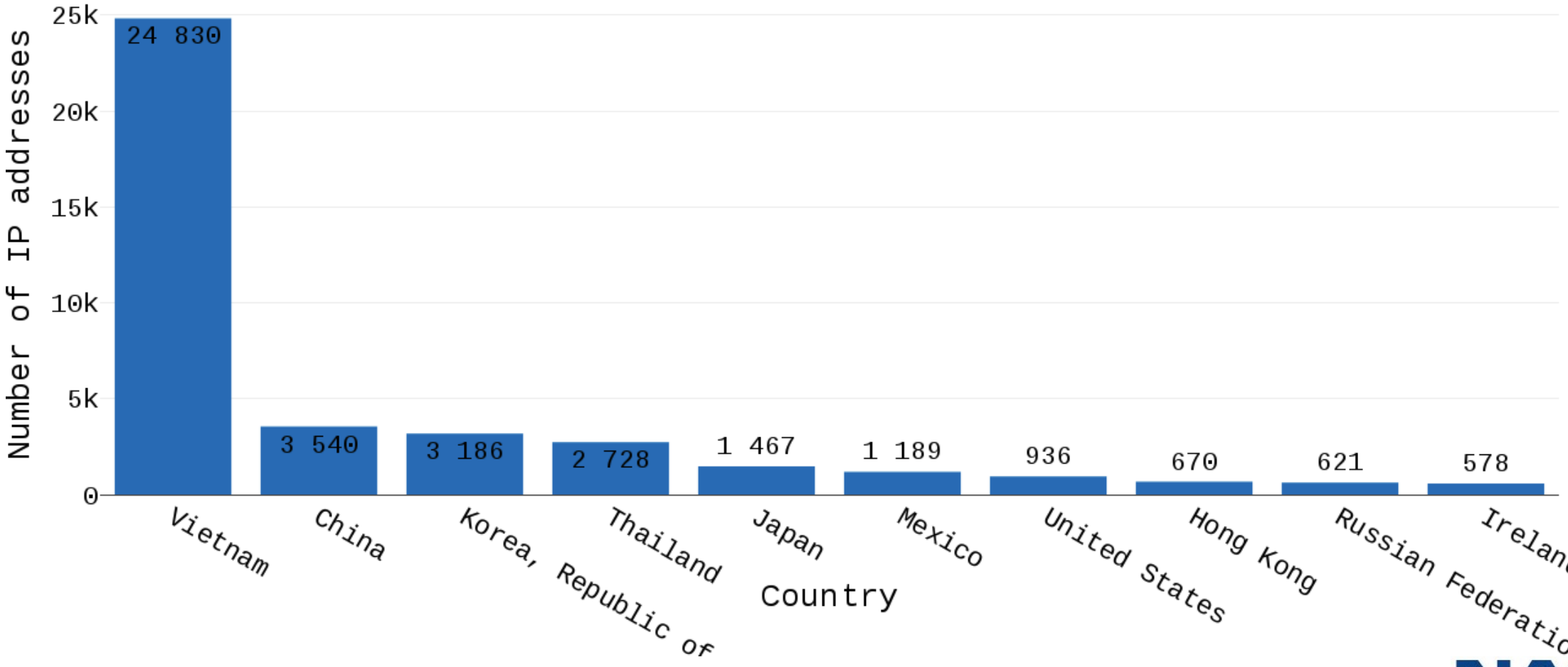


NASK

Botnet fingerprinting

In total, about 45 000 unique IP addresses were identified.

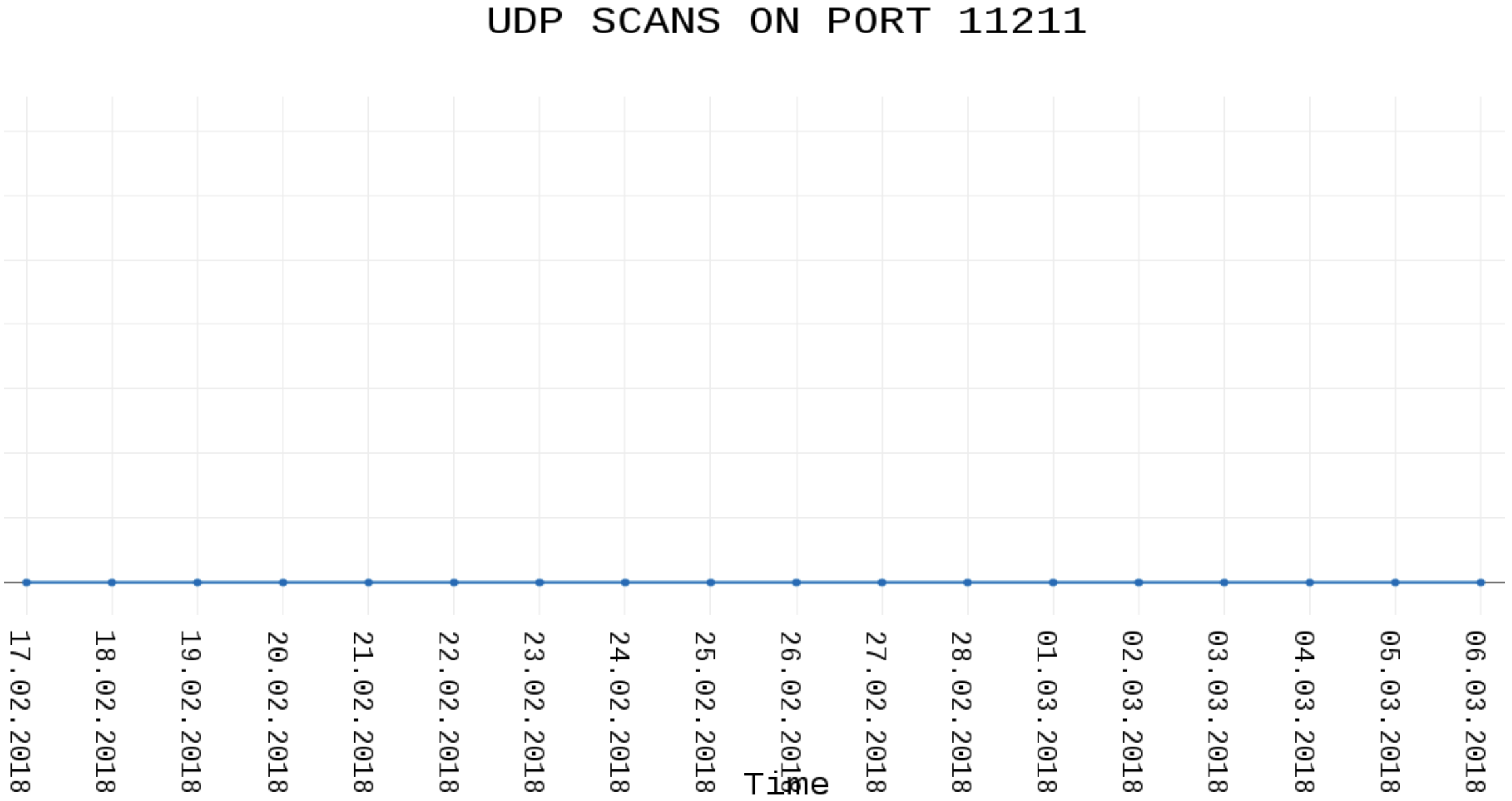
Distribution of source IPs



NASK

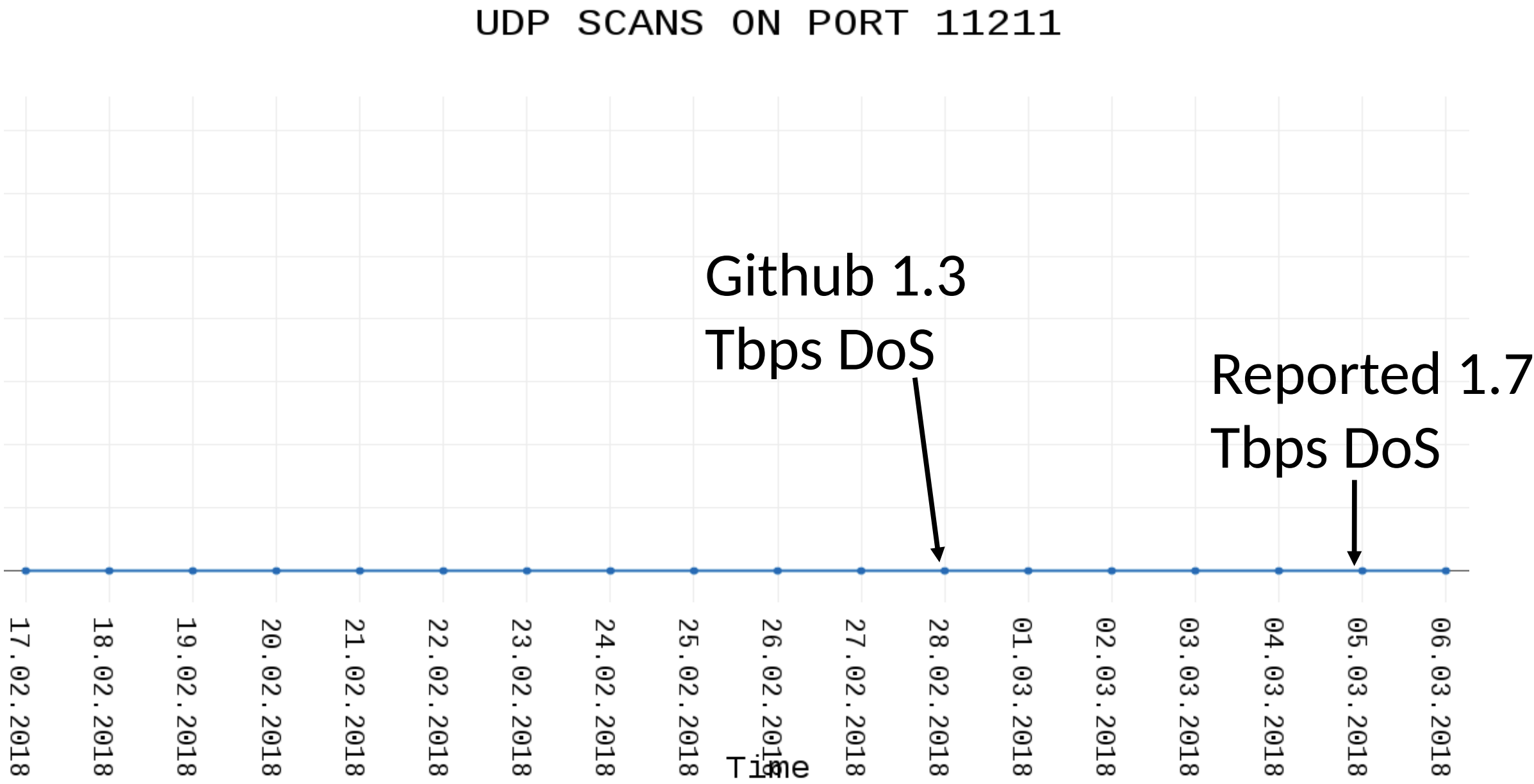
Case study 2
Memcached

Memcached



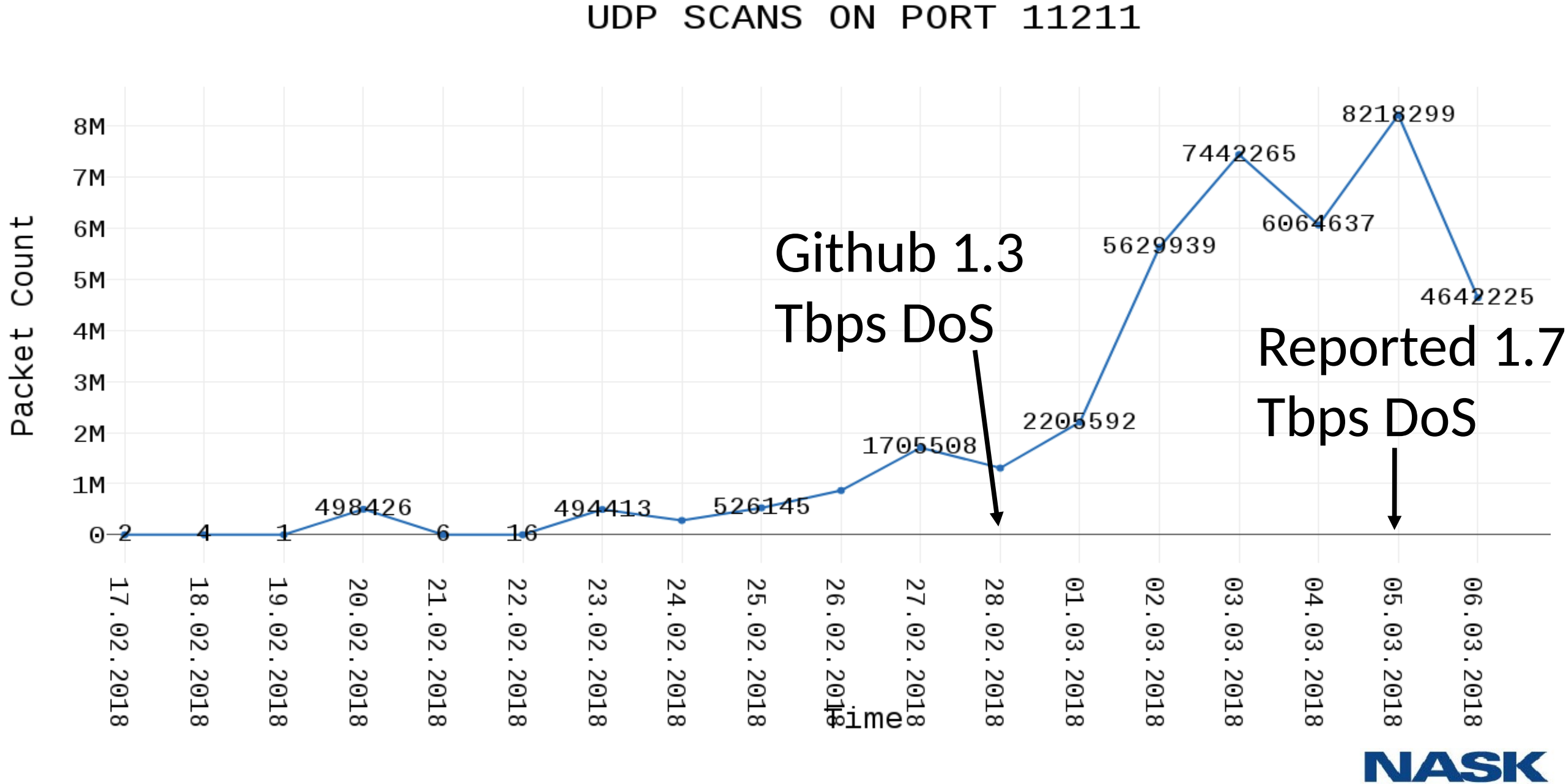
NASK

Memcached



NASK

Memcached



NASK

Day 1 – 20.02 (first scan)

- Only 4 IP addresses
- Source: DigitalOcean, UK
- Duration: 25 minutes
- Constant source port per source IP
- One payload used (memcached statistics)

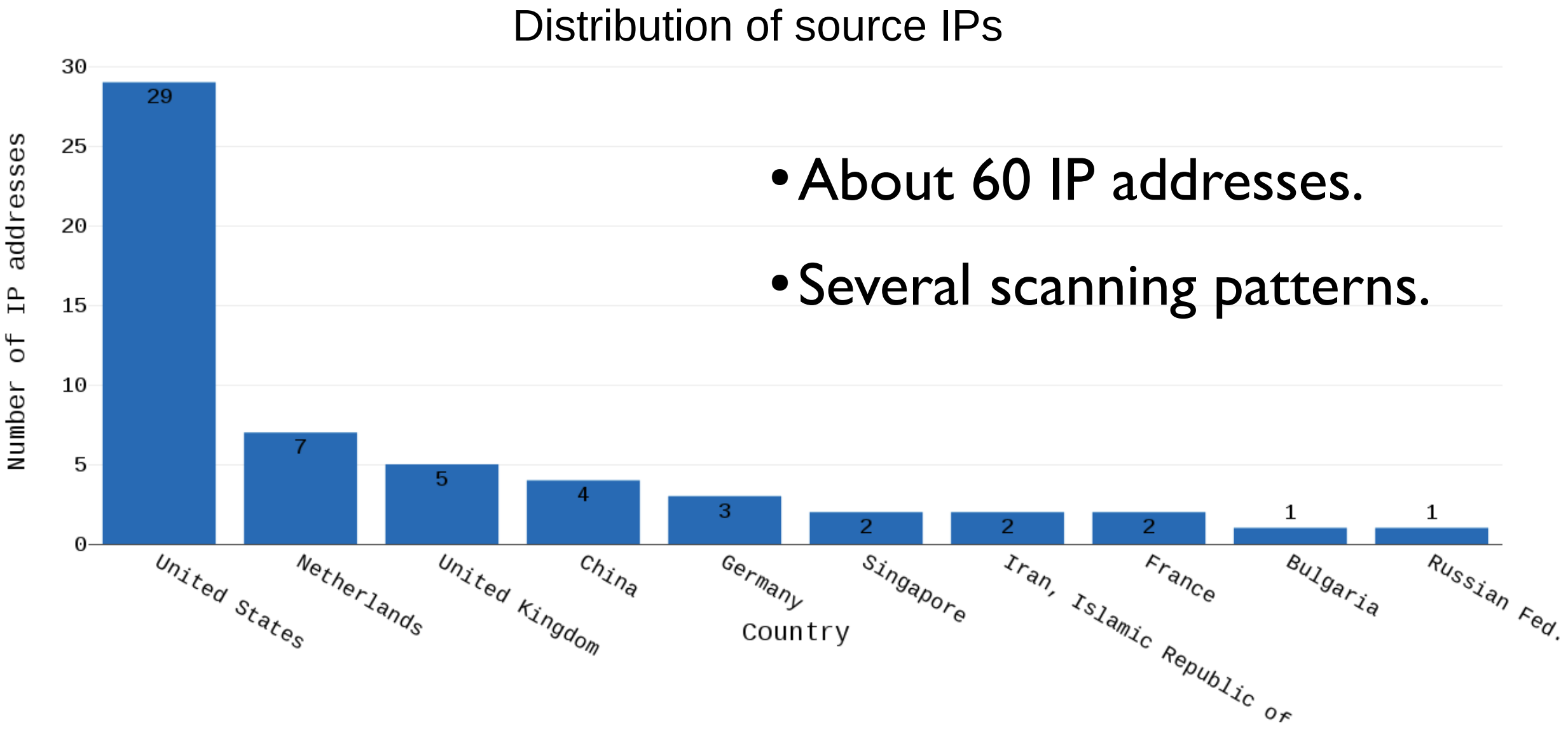
NASK

Day 5 – 24.02 (new actor)

- Only 1 IP addresses
- Source: AS 27176, DataWagon LLC, US
- Small hosting with anti-DDoS
- Randomized source ports
- New payload
- Scan lasted longer: 3 hours

NASK

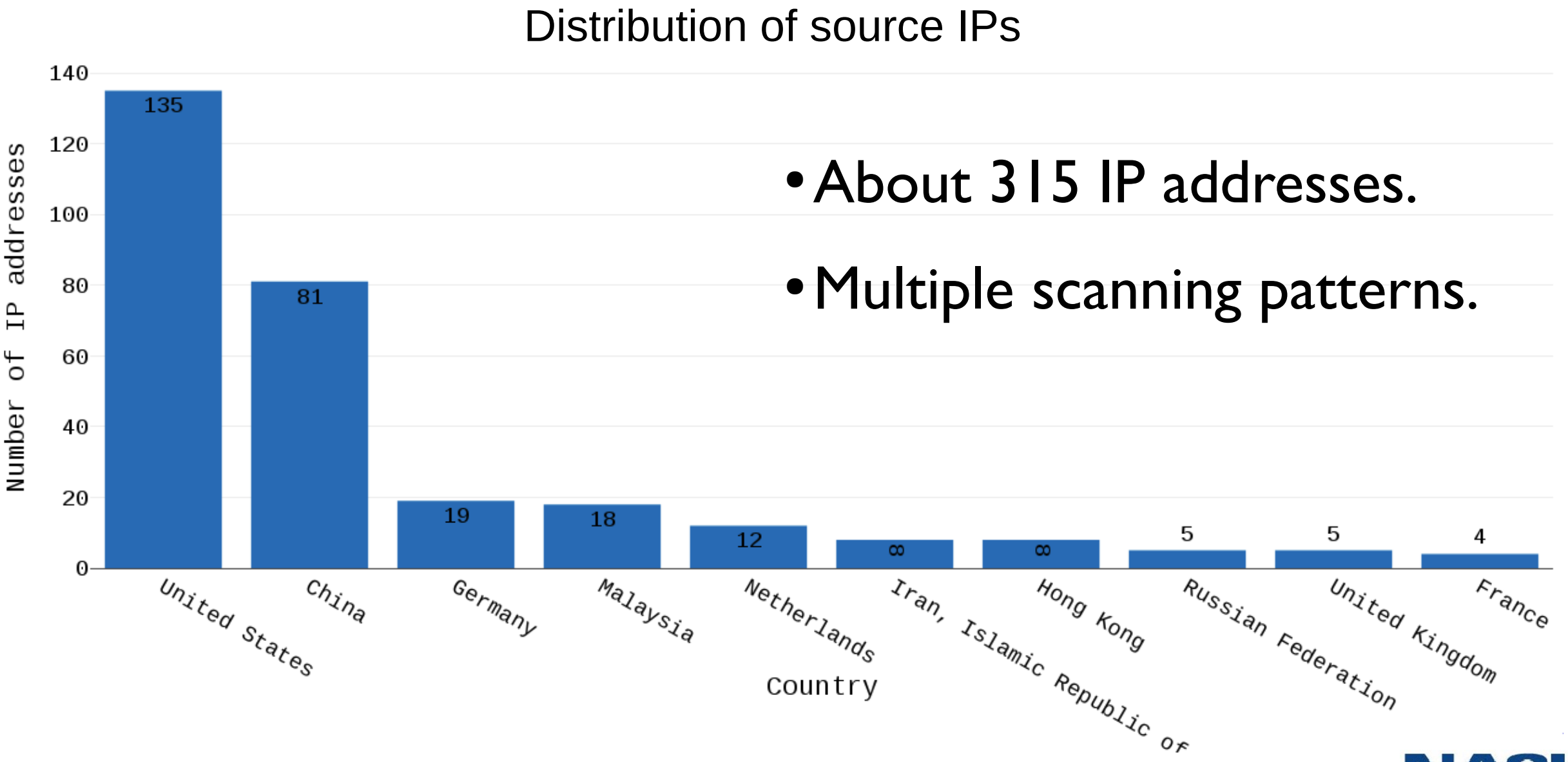
And so on… Pre-GitHub scanners



- About 60 IP addresses.
- Several scanning patterns.

NASK

And so on… Post-GitHub scanners



- About 315 IP addresses.
- Multiple scanning patterns.

NASK

Looking deeper into packets

PGA

- PGA = custom code to generate packets
  - *Improve DDoS Botnet Tracking with Honeypots*, Ya Liu, 360 Netlab, Botconf 4th edition, Dec 2016
- Usually simple operations, examples
  - constant values
  - byte swap
  - incrementation
- Leaves patterns that can be used for IDS
- Our tool detects patterns and creates new signatures

NASK

PGA examples

1. Mirai:

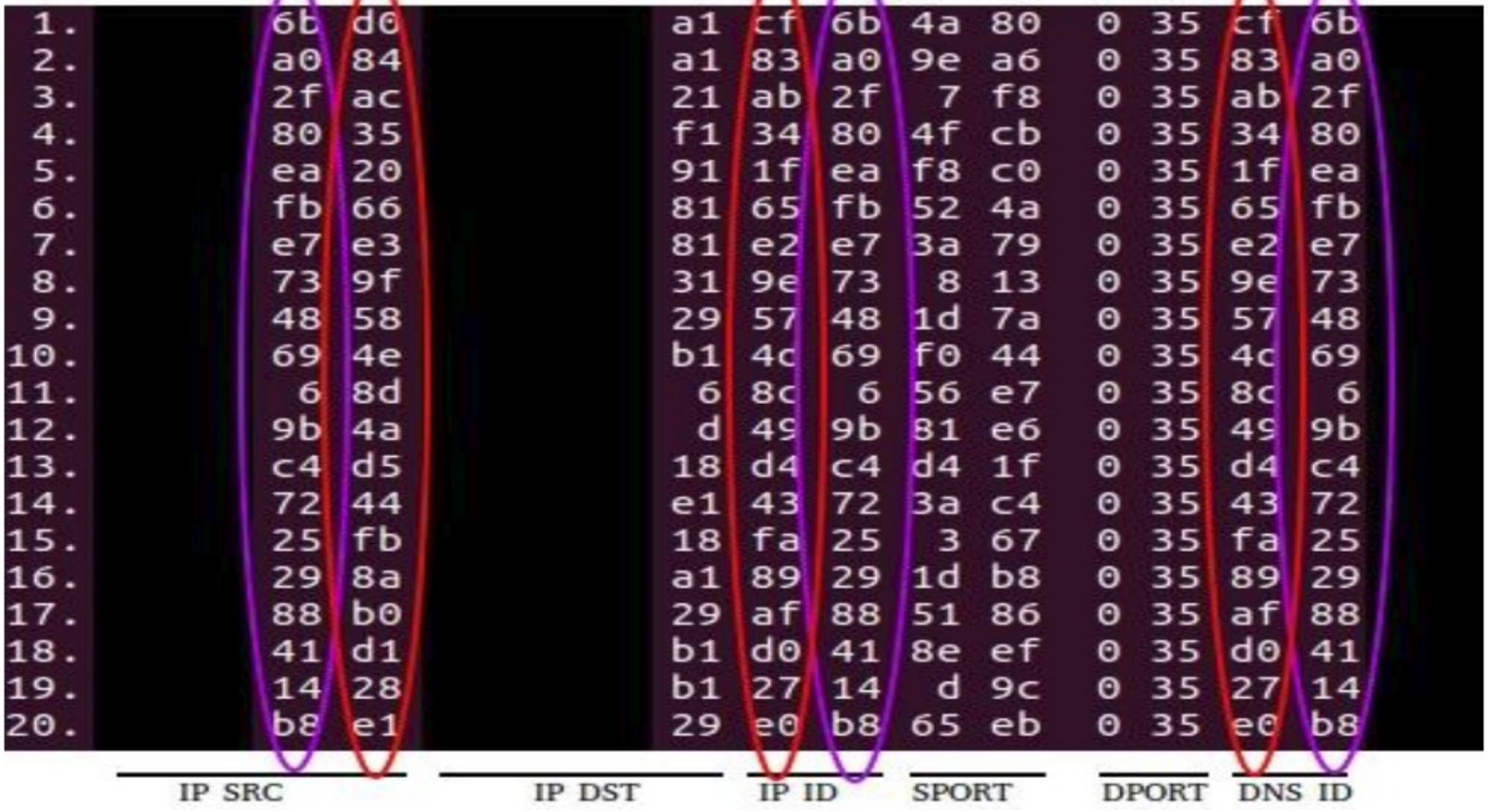
TCP_SEQ = IP_DST

2. XoR.DDoS PGA:

IP_ID = SPORT

TCP_SEQ[1:2] = IP_ID

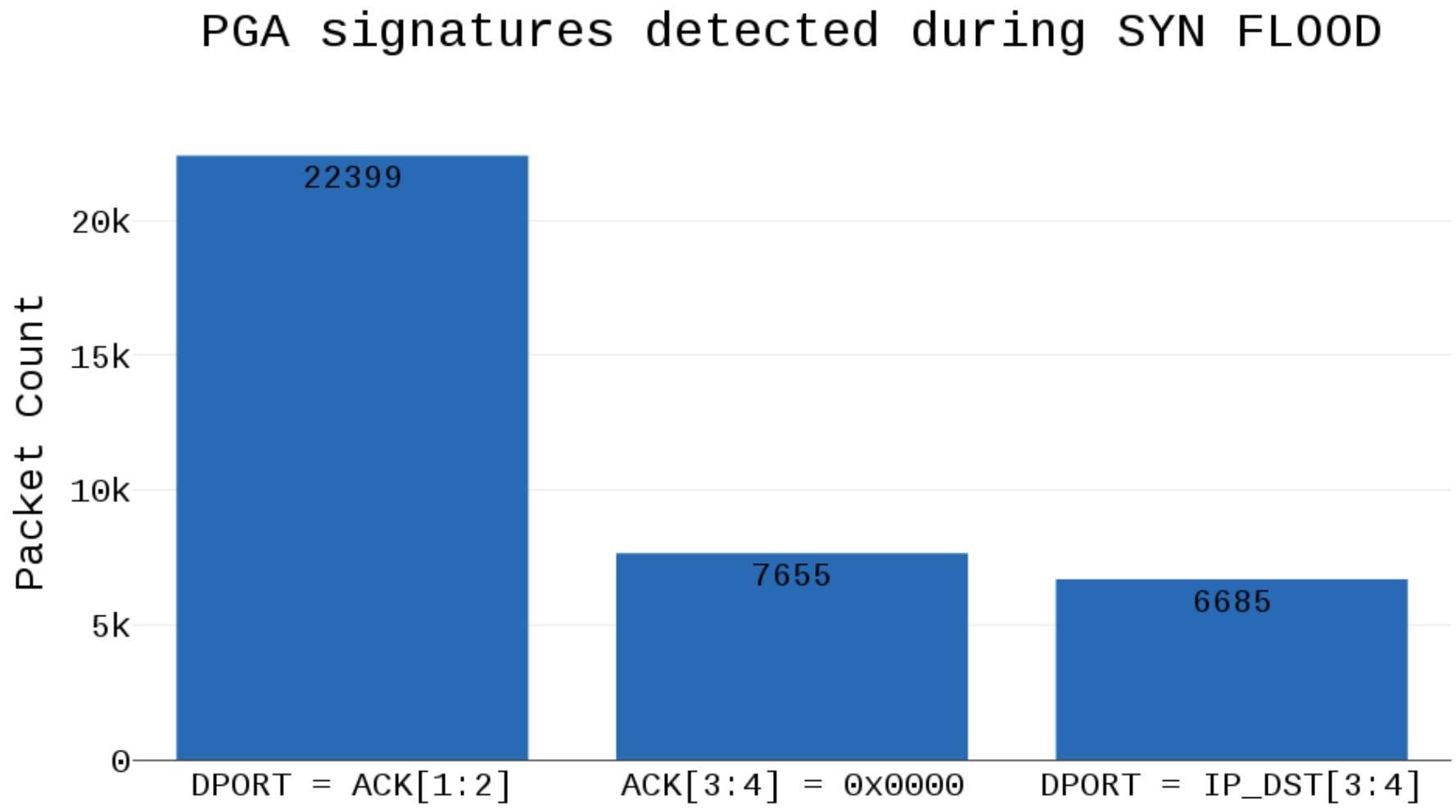
PGA example



NASK

Signatures everywhere

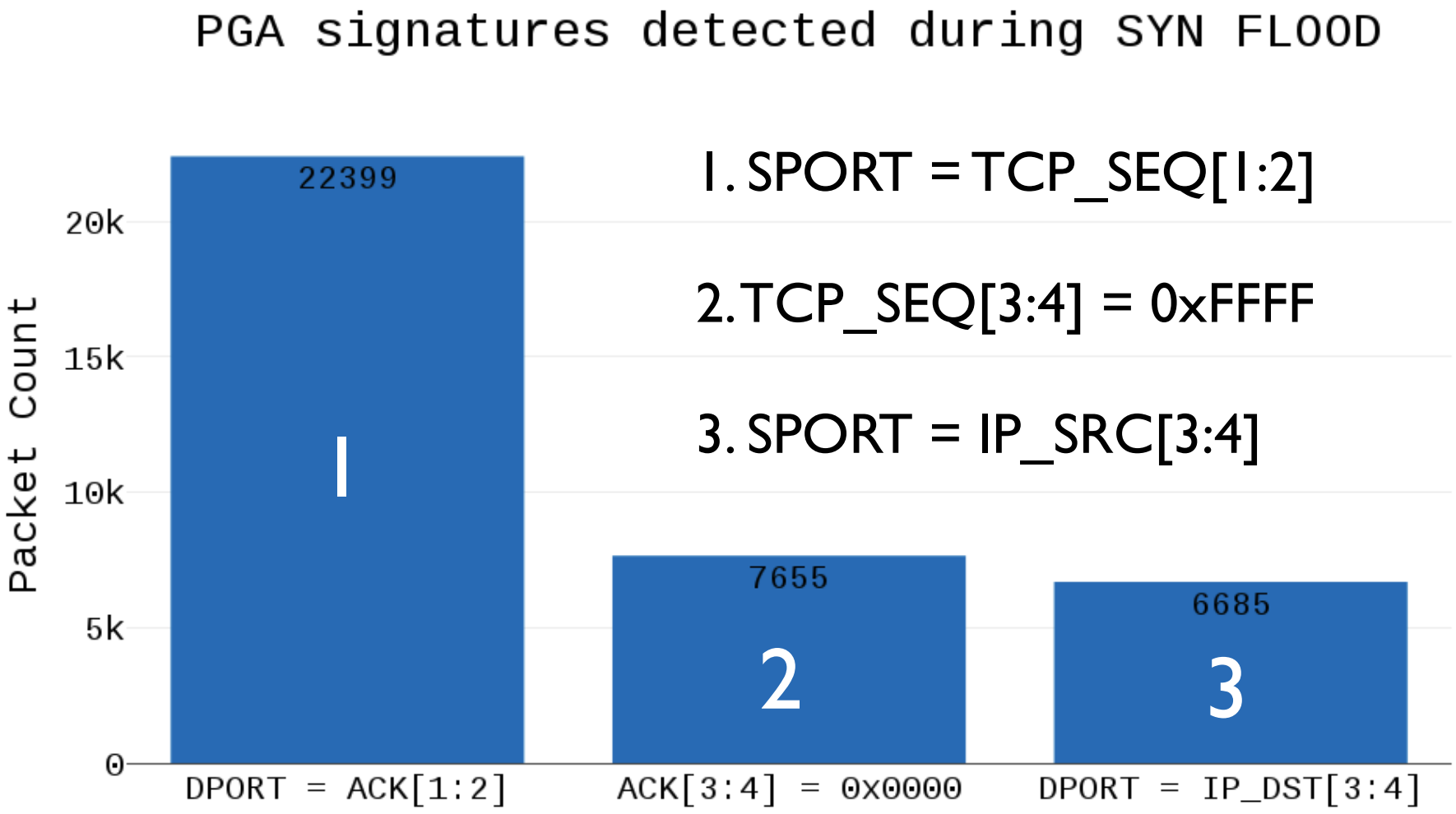
SYN FLOOD on IP belonging to Google – full of PGA signatures.



NASK

Signatures everywhere

SYN FLOOD on IP belonging to Google – full of PGA signatures.



NASK

Operations

Operational value of network telescopes

CERT.PL>_

- Raw output from analyzers is not actionable (too many events)
- **Scans** → abuse notifications (automated for high confidence events)
- **PGA fingerprinting** → Shadowserver remediation feeds
- **DoS attacks** → situational awareness & alerts
- Automated feeds provide limited "intelligence"

NASK

DoS backscatter for the Polish IPv4 space
(color = PGA fingerprint)

Sharing threat information

- Automated distribution of abuse reports & IoCs
- Free
- > 100 active participating entities
- > 50 data sources
- Formats: JSON & CSV & more

NASK

Interested in getting the data?

- Network owners: send an email to n6@cert.pl to sign up
- Usually working with national CSIRTs

NASK

Aiming for actual intelligence

- In-depth analysis of events extracted from the traffic
  - insight into TTP
  - more difficult to automate
- Anomaly / trend detection:
  - forecast exploitation campaigns.
  - new campaigns
- Attribute activities to botnets / actors

NASK

Future plans

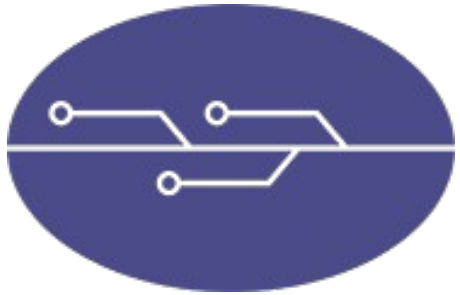
- Combine network telescopes with other data sources

  Honeypots, sandboxes, botnet tracking

- Research collaboration:

  Looking for help in linking PGA signatures to tools / malware

NASK



SISSDEN

https://sissden.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700176.