PARGAV

Privacy Aware Research of Generic Anomalies and Visualisations

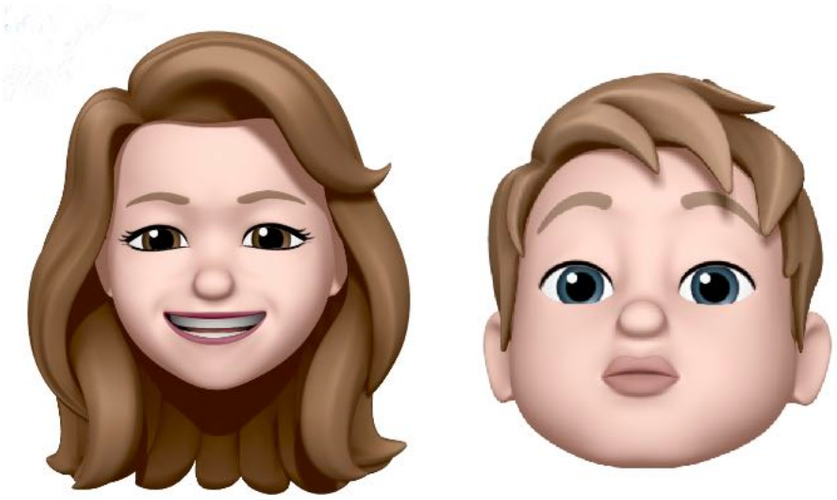
By Anna, Antonios, Grissel, Peter, Petros, Robert, Vasileios

Our Team

PARGAV

Privacy Aware Research of Generic Anomalies and Visualisations

Data Processing



Visualization
Driving

Anomalies
Detection

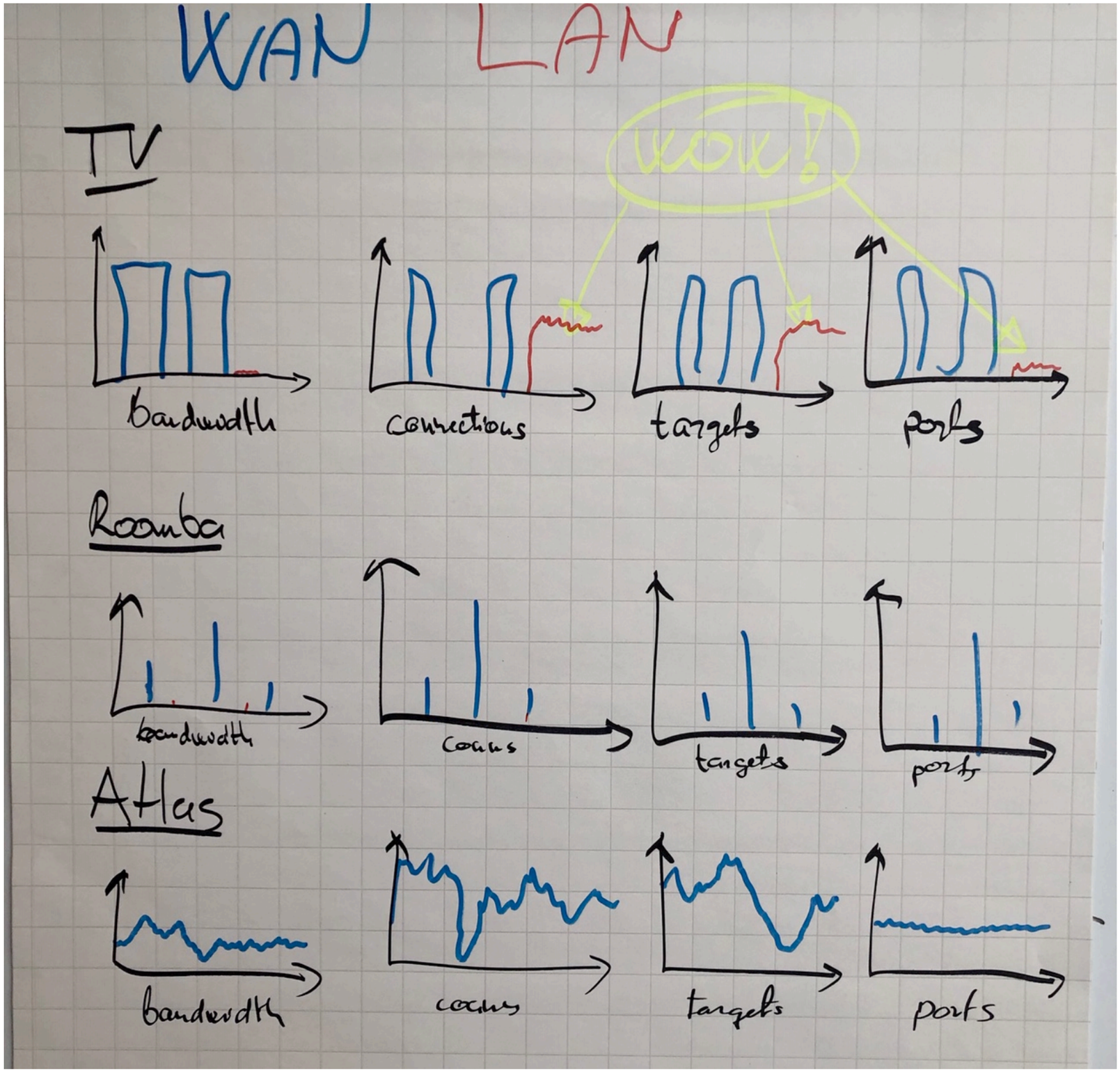
Goal

- Finding methods to identify network anomalies by analysing network traffic patterns.

- Assumption: IoT devices are connected to a (home) network doing their thing. We want to **visualise their behaviour** and **detect anomalies** in network activity.

- **Proof of concept**, based on real-life historical data, some hardly applicable frameworks (visualisation) and needs-a-lot-of-work integrations.

Concept Art


WAN
LAN
TV
wow!
bandwidth
connections
targets
ports
Roomba
bandwidth
counts
targets
ports
Atlas
bandwidth
counts
targets
ports

At a Glance

- Planned to work with real-life, already captured data
- Steps planned:
    1. Pre-processing
    2. Graphing
    3. Anomaly detection
        A. Naïve
        B. “Professional”
        C. Perhaps both
    4. Future work: categorise, learn traffic patterns, adapt, block, …

Data preparation

- In real life scenarios one does real-time pcaps, monitor (DHCP) clients, … to produce streamed input
- Now we “replayed” existing data, converted it to fit graphing / anomaly detection

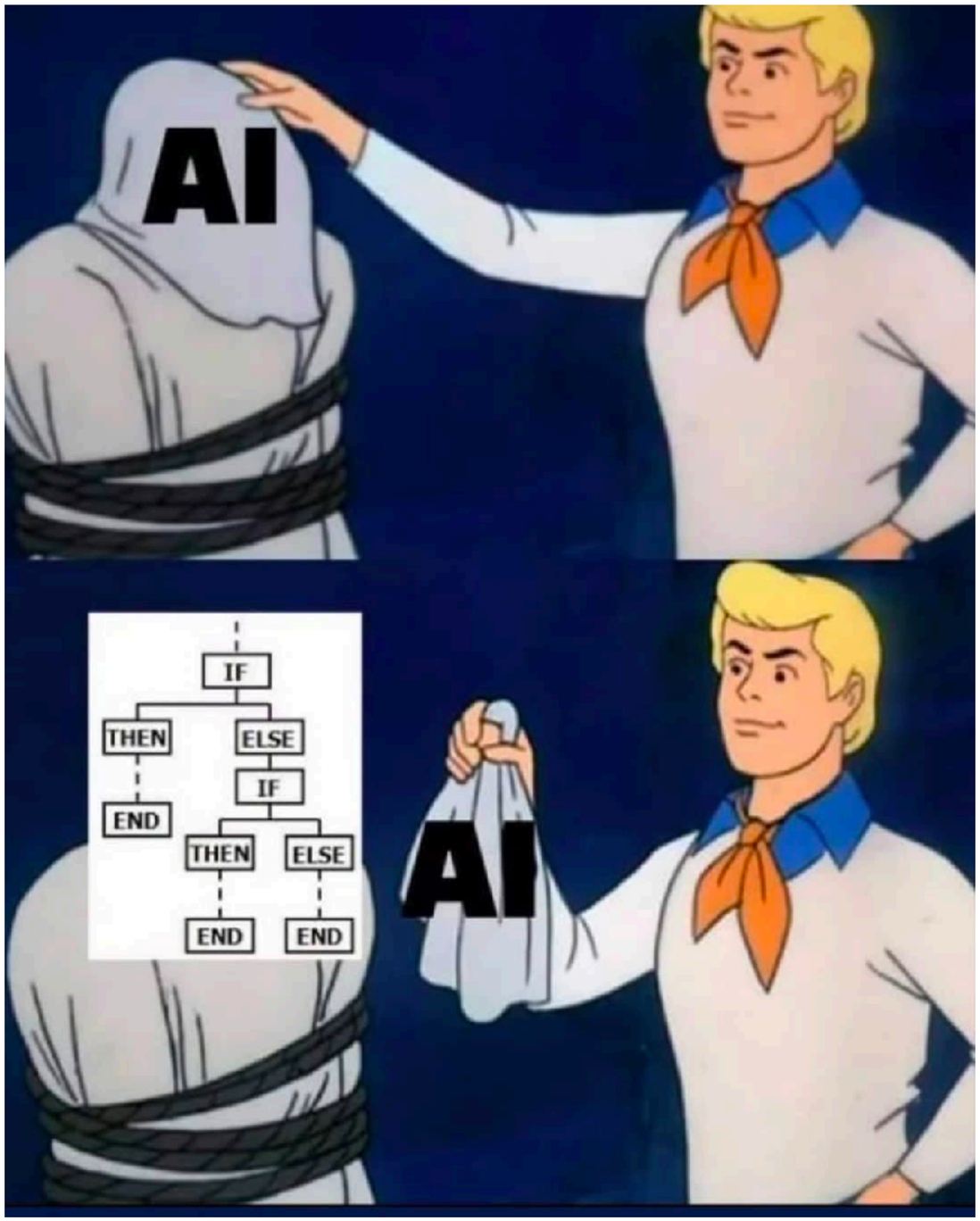
Graphing

- Could be done with RRD on constrained devices
- Maybe Grafana, InfluxDB, … in less constrained environments
- We visualised historical data, went with something simpler (d3js/c3js)
-

Anomaly Detection

- Naïve approach:
    - Compare current values to median / average of past few minutes / hours
- Professional tools:
    - luminol (https://github.com/linkedin/luminol) &
    - prophet (https://facebook.github.io/prophet/docs/quick_start.html)
- In real life combinations are possible (ie. naive detector has a signal, sends data off for confirmation to a different algorithm)

Anomaly Detection



Other ideas

- Categorise devices
    - A TV behaves differently (ie. has different traffic patterns) than a Roomba or a phone or a RIPE Atlas probe
- “Learning/training mode” to establish normal behaviour
-

Data Used

- Mon(IoT)r Testbed
  - https://moniotrlab.ccis.neu.edu/tools/
- Also looked at BaIoT attack data:
  - https://archive.ics.uci.edu/ml/machine-learning-databases/00442/

Data Used

Selecting IoT Devices

- **Criteria**: category; features; popularity; US & UK markets

Flux Bulb
Xiaomi Strip
Philips Bulb
LG TV
Amazon Cam
Invoke Speaker
Amcrest Cam
Behmor Brewer
Lefun Cam
GE Microwave
Luohe Cam
Samsung Dryer
Micro7 Cam
Samsung Fridge
ZModo Bell
Samsung Washer
Wink2 Hub
Smarter iKettle
D-Link Sensor
Xiaomi Rice Cooker

N=46

Blink Cam
Blink Hub
Ring Doorbell
Wanswiew Cam
Yi Cam
Insteon Hub
Lightify Hub
Philips Hue Hub
Sengled Hub
Smartthings Hub
Xiaomi Hub
Magichome Strip
Nest T-stat
TP-Link Bulb
TP-Link Plug
WeMo Plug
Apple TV
Fire TV
Roku TV
Samsung TV
Echo Dot
Echo Spot
Echo Plus
Google Home Mini
Anova Sousvide
Xiaomi Cleaner

N=26

Bosiwo Cam
D-Link Cam
WiMaker Cam
Xiaomi Cam
Honeywell T-stat
Allure Speaker
Google Home
Netatmo Weather
Smarter Brewer

N=35

20 Cameras	13 Smart Hubs	15 Home Automation	9 TVs	11 Speakers	13 Appliances	81 Total

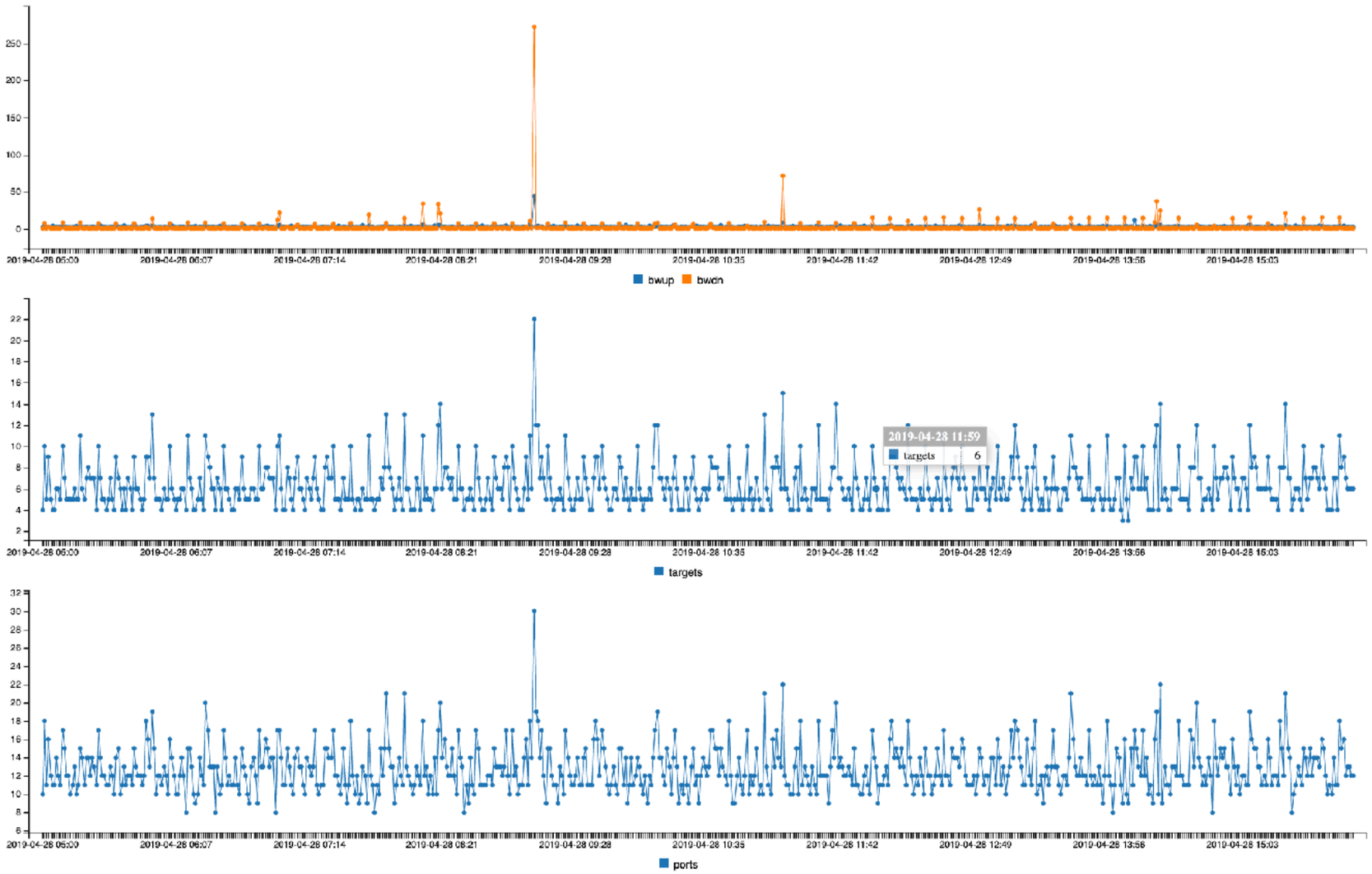




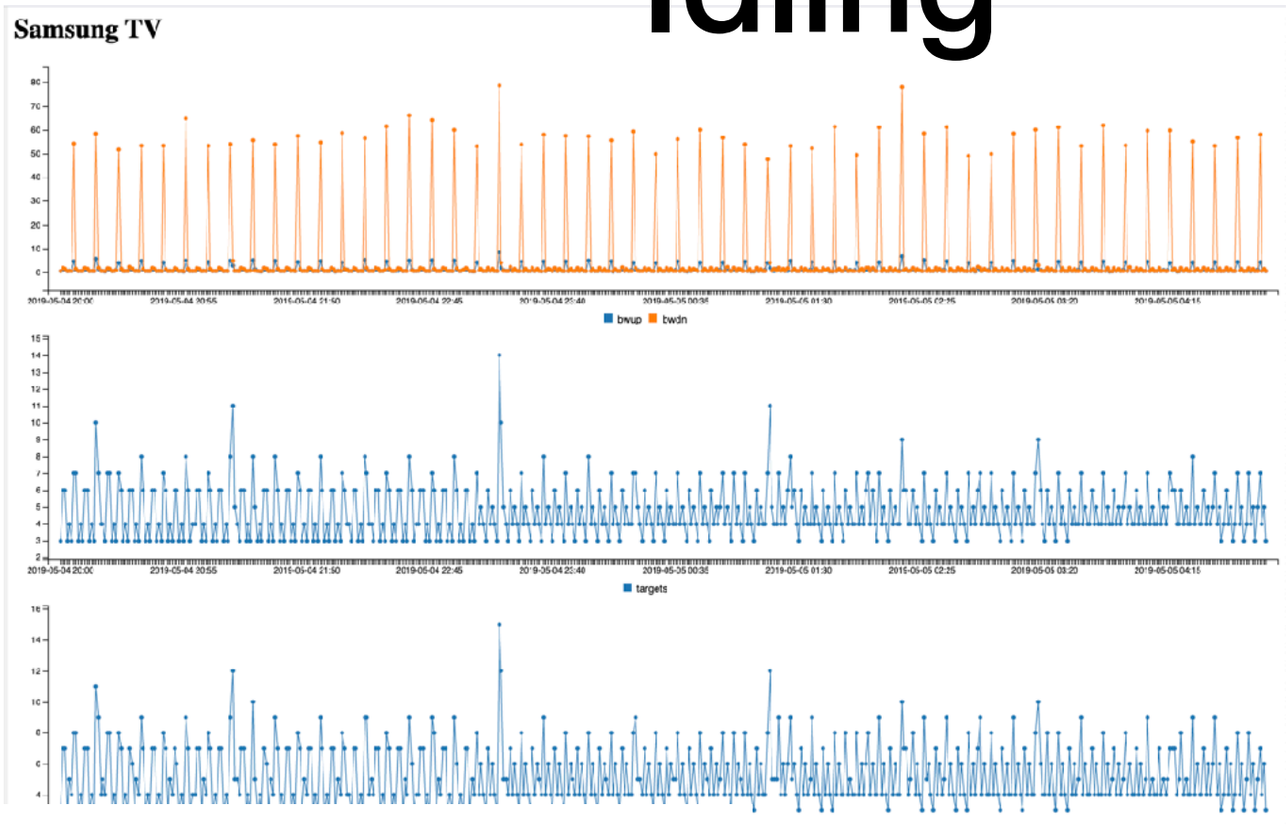


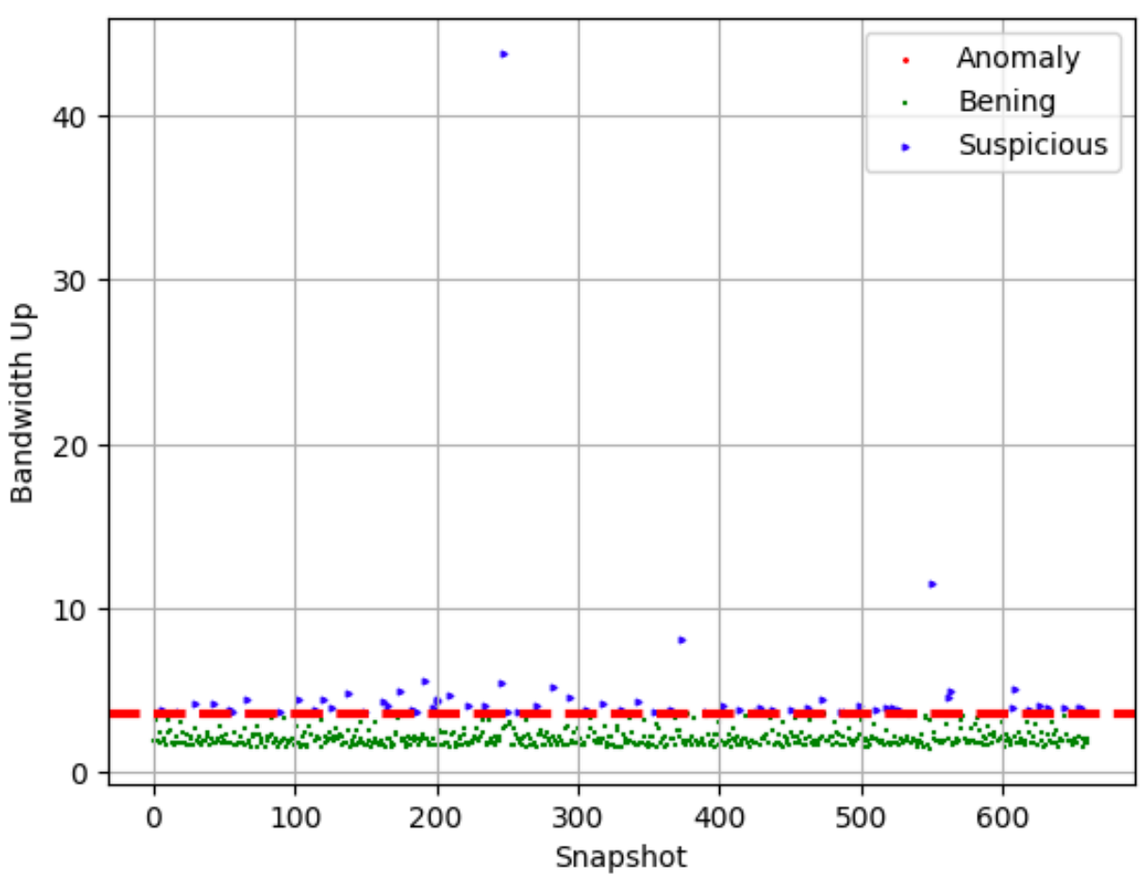
Idling

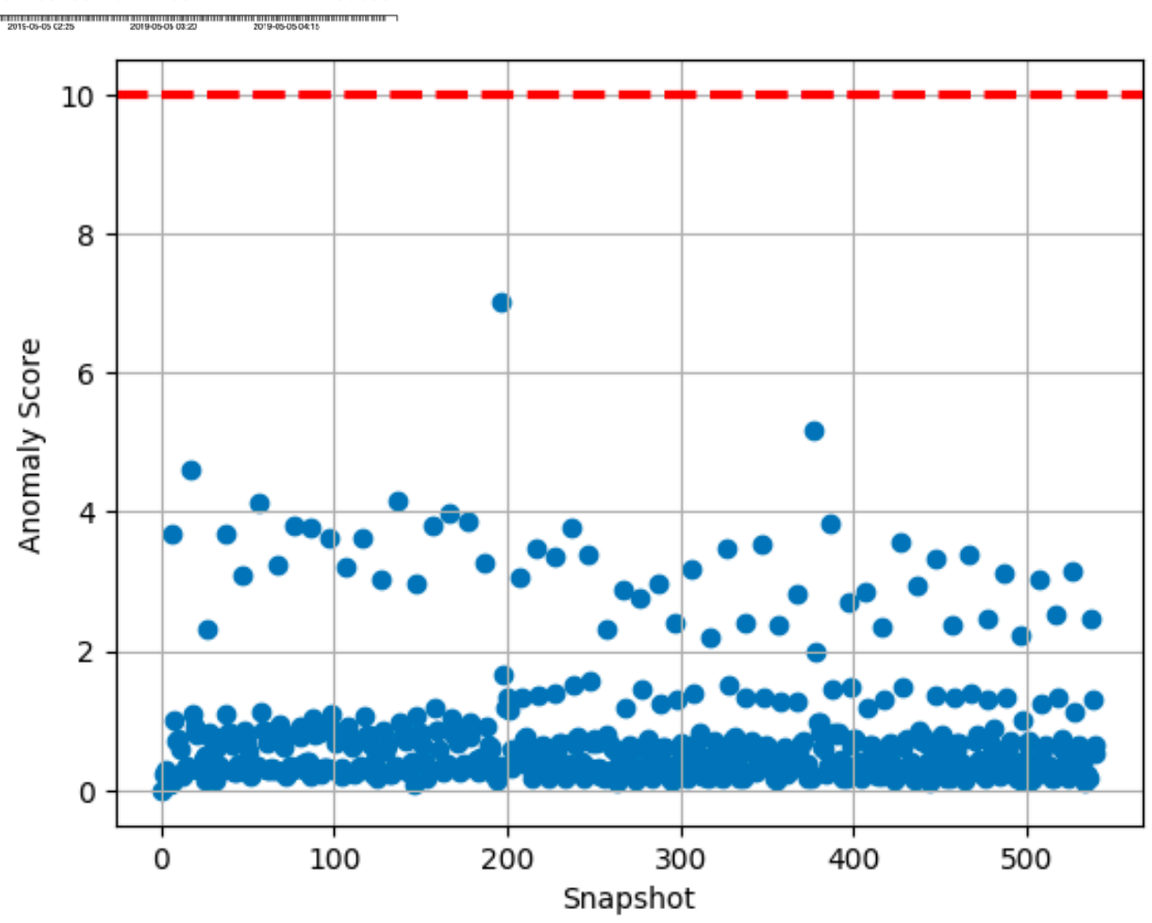
Samsung TV (US)



Idling

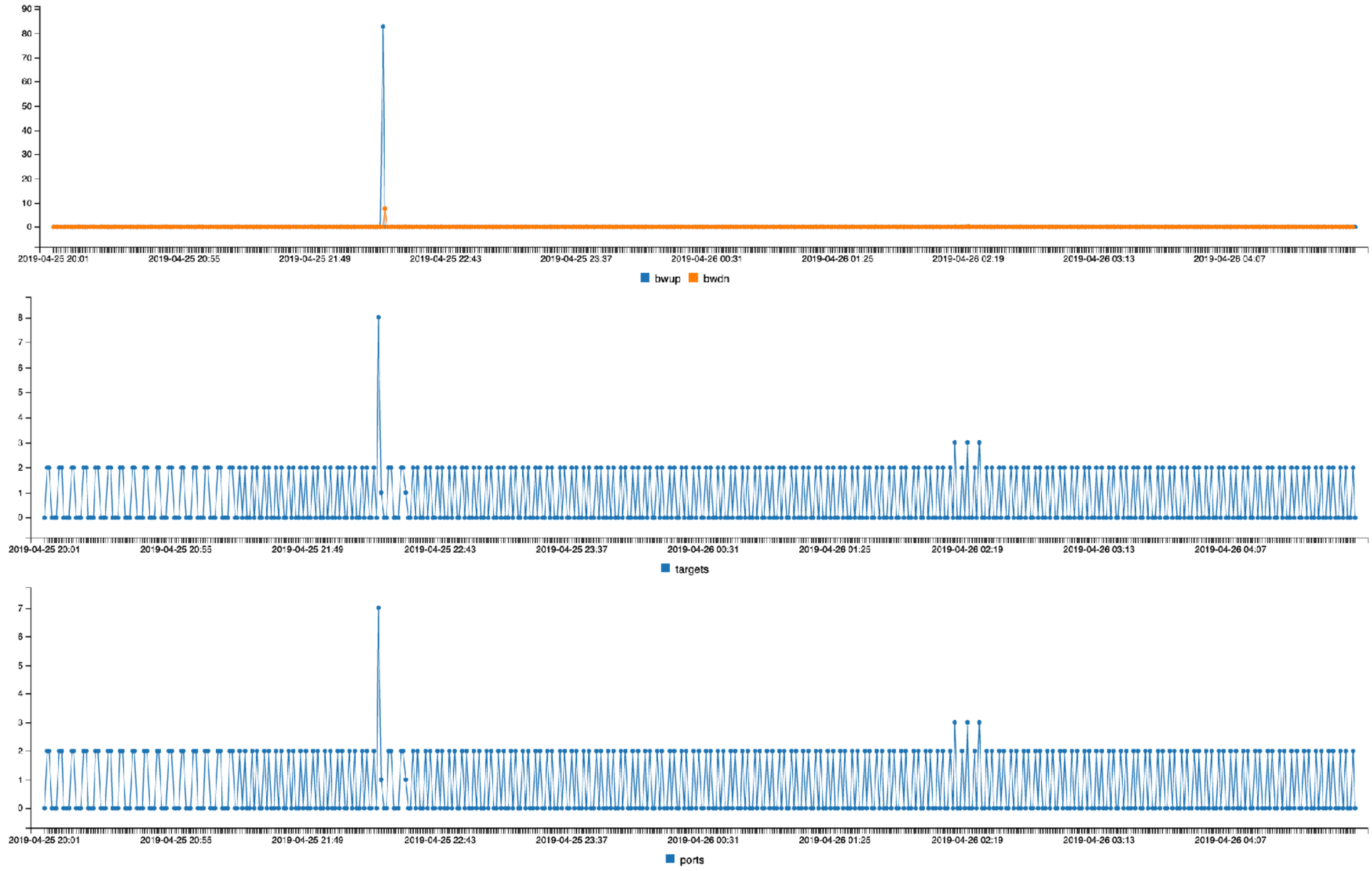

Samsung TV
bwup
bwdn
targets


Anomaly
Bening
Suspicious
Bandwidth Up
Snapshot


Anomaly Score
Snapshot

Idling

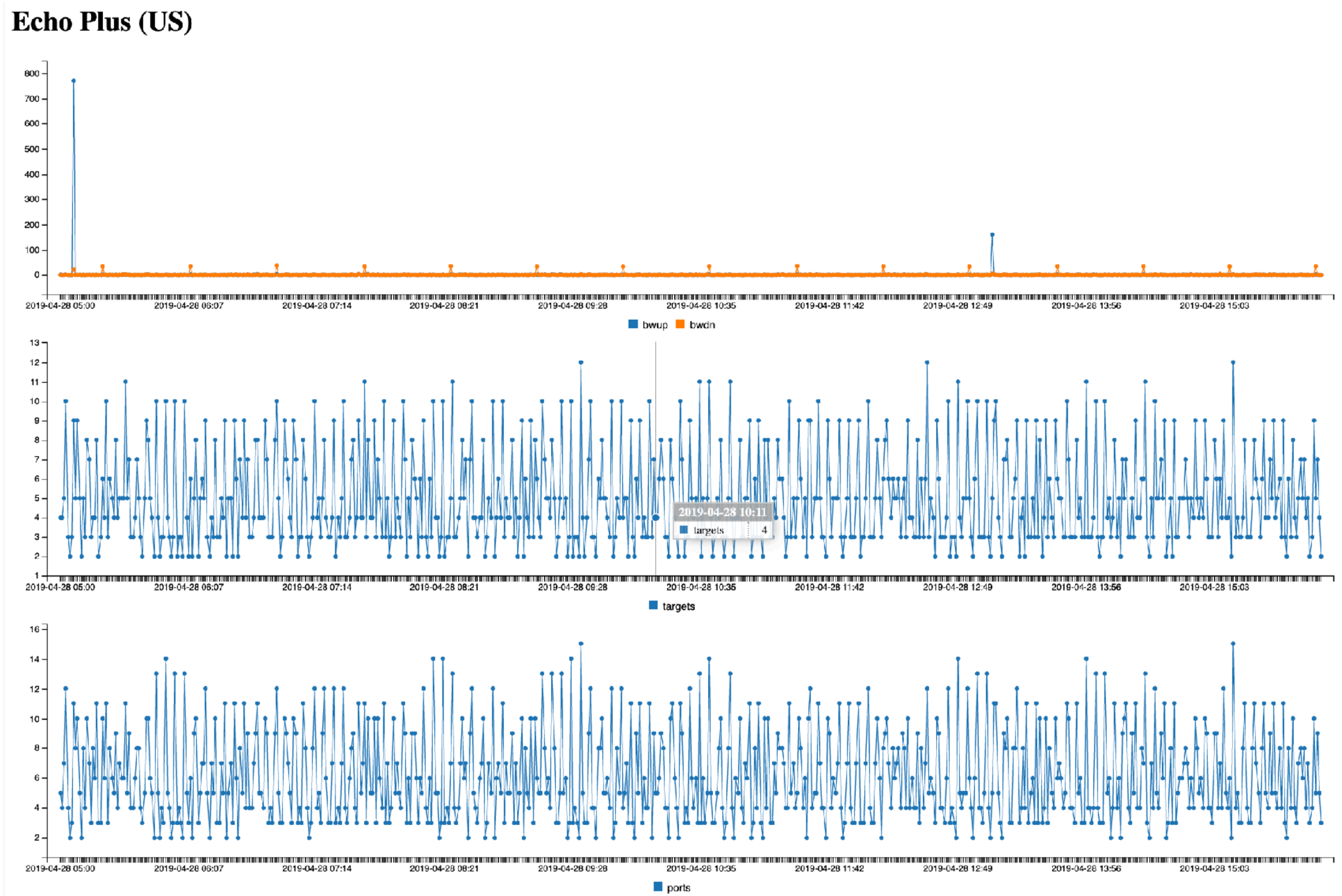
Ring


90
80
70
60
50
40
30
20
10
0
2019-04-25 20:01
2019-04-25 20:55
2019-04-25 21:49
2019-04-25 22:43
2019-04-25 23:37
2019-04-26 00:31
2019-04-26 01:25
2019-04-26 02:19
2019-04-26 03:13
2019-04-26 04:07
bwup
bwdn

8
7
6
5
4
3
2
1
0
2019-04-25 20:01
2019-04-25 20:55
2019-04-25 21:49
2019-04-25 22:43
2019-04-25 23:37
2019-04-26 00:31
2019-04-26 01:25
2019-04-26 02:19
2019-04-26 03:13
2019-04-26 04:07
targets

7
6
5
4
3
2
1
0
2019-04-25 20:01
2019-04-25 20:55
2019-04-25 21:49
2019-04-25 22:43
2019-04-25 23:37
2019-04-26 00:31
2019-04-26 01:25
2019-04-26 02:19
2019-04-26 03:13
2019-04-26 04:07
ports

Idling


Echo Plus (US)
800
700
600
500
400
300
200
100
0
2019-04-28 05:00
2019-04-28 06:07
2019-04-28 07:14
2019-04-28 08:21
2019-04-28 09:28
2019-04-28 10:35
2019-04-28 11:42
2019-04-28 12:49
2019-04-28 13:56
2019-04-28 15:03
bwup
bwdn
13
12
11
10
9
8
7
6
5
4
3
2
1
2019-04-28 10:11
targets 4
targets
16
14
12
10
8
6
4
2
ports

Attaaaaaaaack!