DEFENDING RPKI

DKNOG15

Job Snijders

AGENDA

01 THREATS TO RPKI

02 HIDING IN THE CROWD

03 PRELIMINARY RESULTS

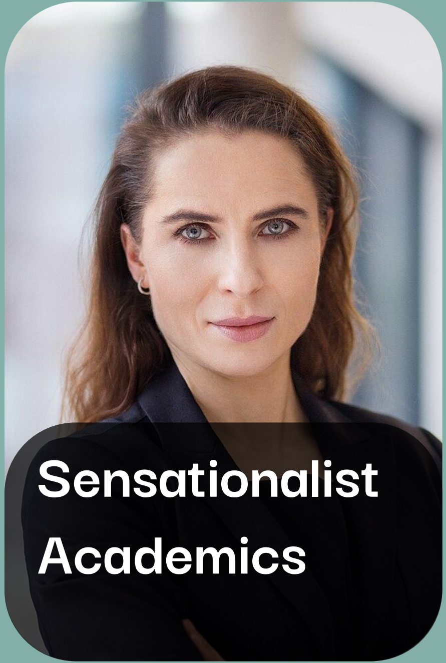
04 THE PLAN

05 QUESTIONS

THREATS TO RPKI

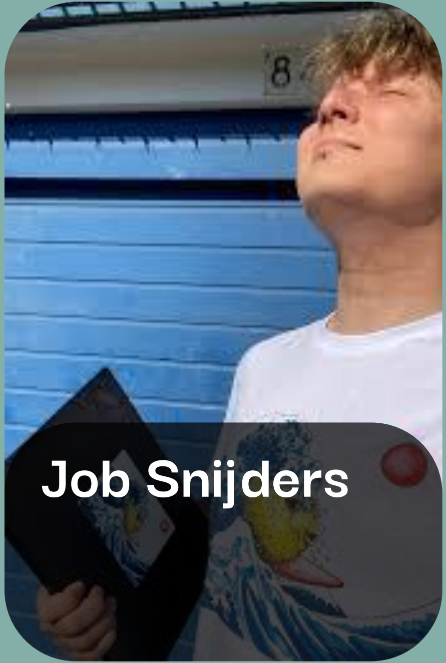
1

MEET THE TEAM



Sensationalist Academics

Unethical Hackers



Job Snijders

Well meaning Operators

THINGS I WORRY ABOUT

- Crashing validators
- System compromise via validators
- Operators disabling RPKI “because RPKI itself seems a risk”
- The clock on Internet routing security turning back

HIDING IN THE CROWD

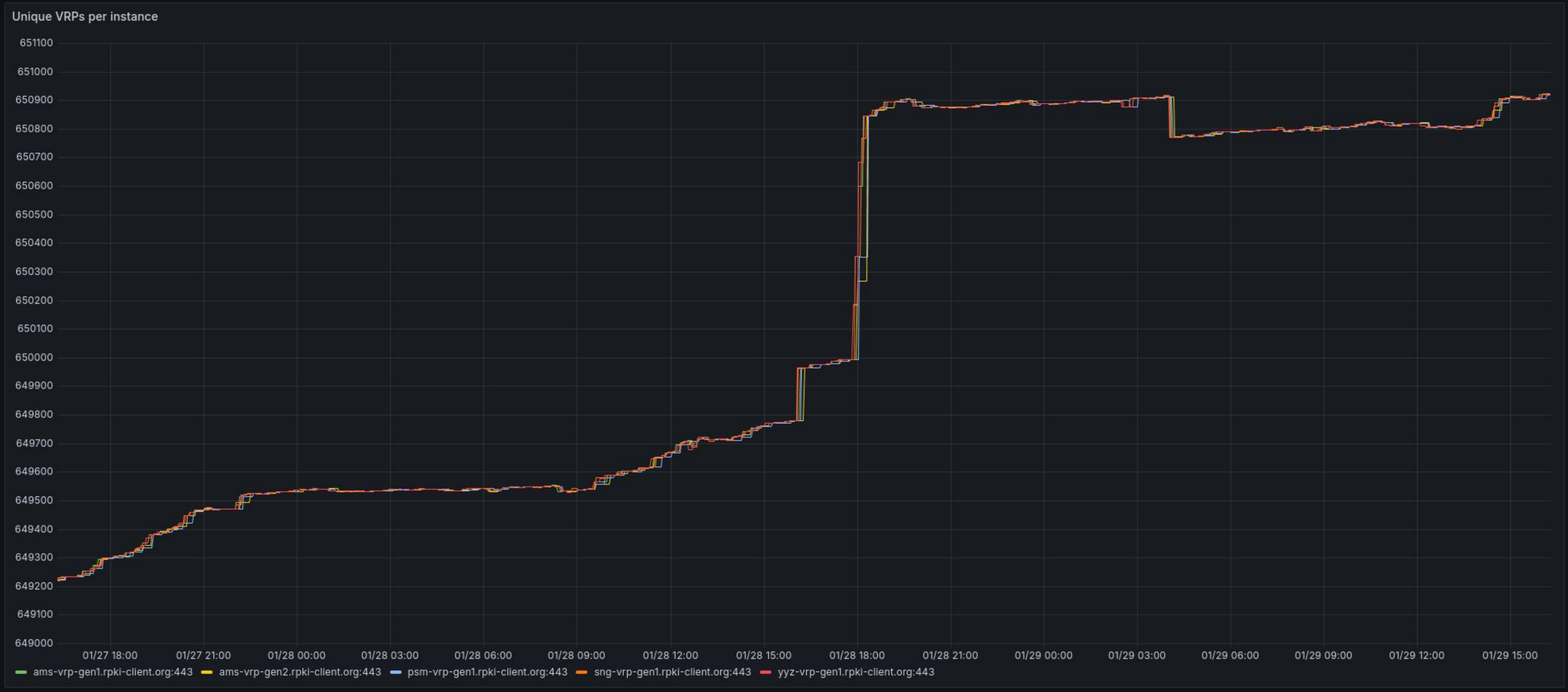
2

HIDING RPKI VALIDATORS

- Publication point operators don’t need to know the source IP addresses of validators, do they?

PRELIMINARY RESULTS

3


Unique VRPs per instance
651100
651000
650900
650800
650700
650600
650500
650400
650300
650200
650100
650000
649900
649800
649700
649600
649500
649400
649300
649200
649100
649000
01/27 18:00
01/27 21:00
01/28 00:00
01/28 03:00
01/28 06:00
01/28 09:00
01/28 12:00
01/28 15:00
01/28 18:00
01/28 21:00
01/29 00:00
01/29 03:00
01/29 06:00
01/29 09:00
01/29 12:00
01/29 15:00
ams-vrp-gen1.rpki-client.org:443
ams-vrp-gen2.rpki-client.org:443
psm-vrp-gen1.rpki-client.org:443
sng-vrp-gen1.rpki-client.org:443
yyz-vrp-gen1.rpki-client.org:443

PRELIMINARY RESULTS

- No significant difference between anonymized and exposed RPs
- RRDP-via-overlay not as reliable as “direct”
  - As long as “direct” is used as fallback, no difference

THE PLAN

4

PLAN: AREA OF STUDY

- Does use of *forward proxies* at scale work well for the RPKI?
- How to handle transport switch-overs?
- Set up more experiments

REQUEST TO YOU

- I need VPS/Compute/Storage resources to run experiments

QUESTIONS?

5

THANK YOU

Job Snijders

job@sobornost.net