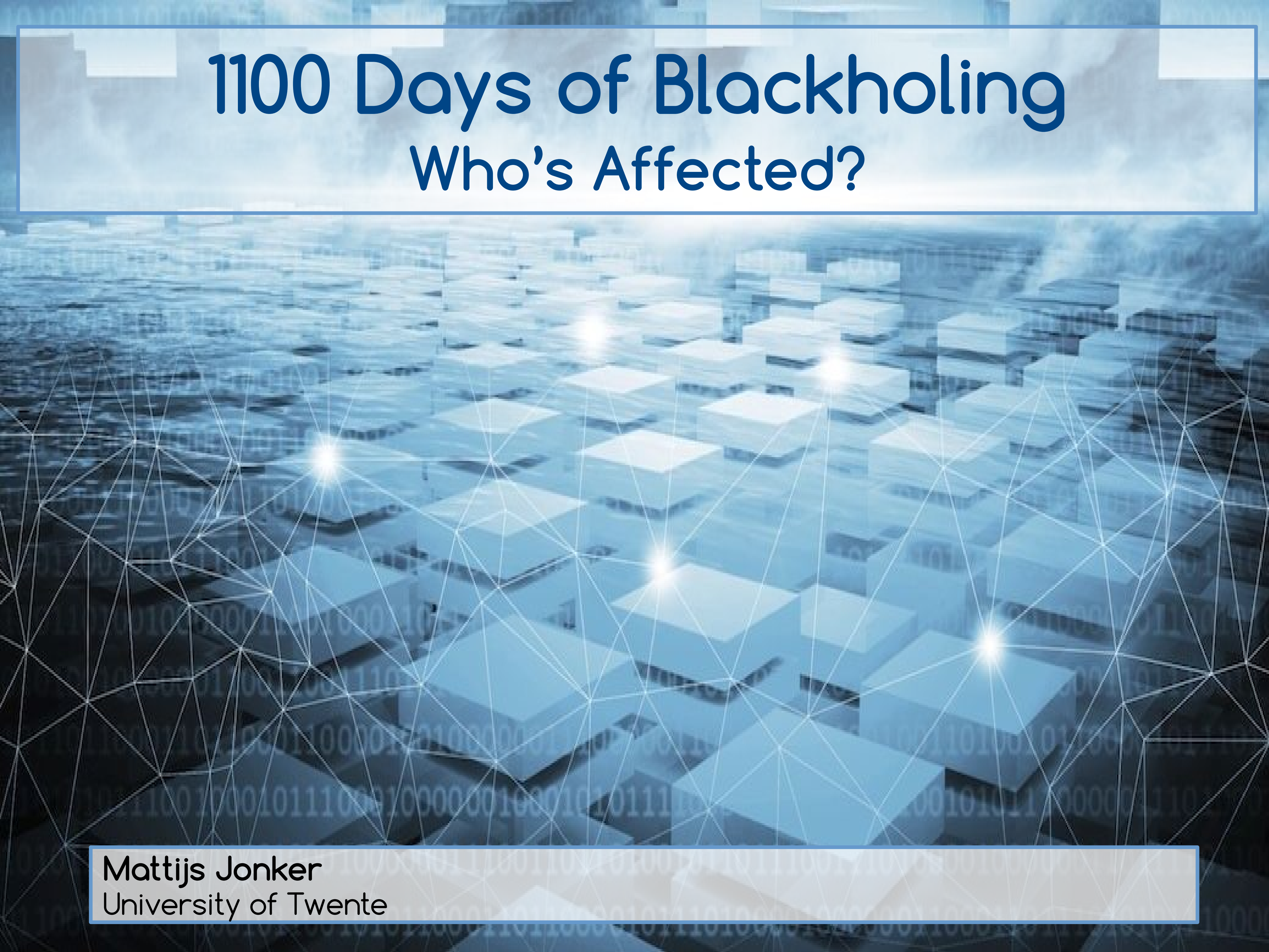
1100 Days of Blackholing

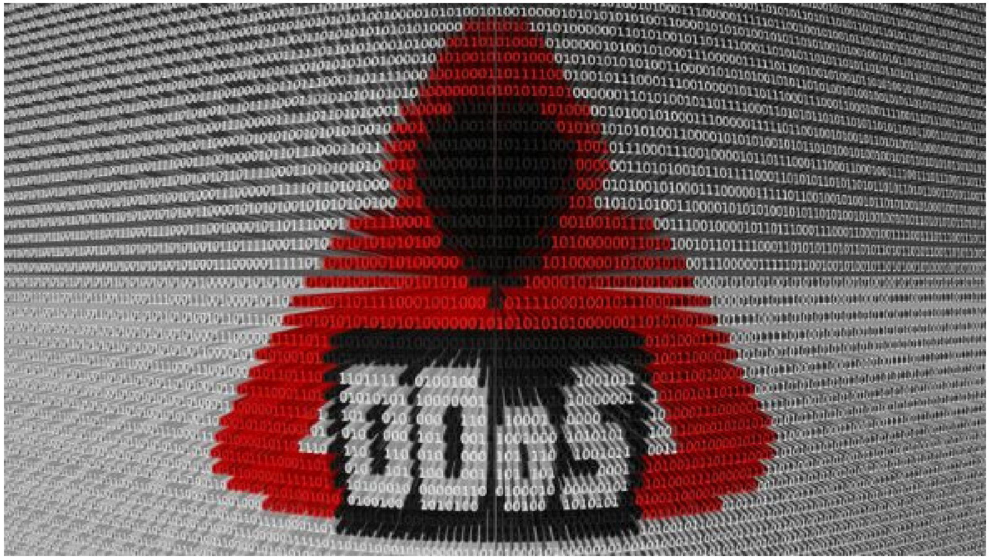
Who's Affected?



Mattijs Jonker
University of Twente

Denial-of-Service (DoS) attacks

- Simple, yet effective class of attacks
- Have gained a lot in popularity over the last years
- Offered "as-a-Service" to the layman for only a few USD



Data sets

- In an IMC 2017 paper[1] we put together global Internet measurement infrastructures:
  - A large network telescope (UCSD-NT)
  - Logs from amplification honeypots (AmpPot)
  - Data from large-scale, active DNS measurements (OpenINTEL)
- This allowed us to characterize attacks, attacked IP targets, and DDoS Protection Services

[1] M. Jonker, A. Dainotti and others, Millions of Targets Under Attack: a Macroscopic Characterization of the DoS Ecosystem, In IMC’17.

UCSD Network Telescope

- A /8 darknet
- Captures DoS attacks with randomly (and uniformly) spoofed IP addresses
- Captures ~1/256th of IPv4 address space
- Any sizable attack should be visible

Amplification honeypot (AmpPot)

- Honeypot that mimicks reflectors
  - various protocols (e.g., NTP, DNS, and CharGen)
- Tries to be appealing to attackers
  - i.e., by offering large amplification
- Twenty-four AmpPot instances
  - Geographically & logically distributed

Attack events coverage

- We analyze two years of attack traces
  - March 1, 2015 – Feb 28, 2017
- The attacks data sets complement each other:
  - honeypots don't register randomly spoofed attacks
  - a darknet doesn't register reflection attacks
- But we don't see all attacks

(Any ideas / suggestions for additional data?)

A glimpse at our findings

source	#events	#targets	#/24s	#ASNs
UCSD-NT	12.47M	2.45M	0.77M	25990
AmpPot	8.43M	4.18M	1.72M	24432
	20.90M	6.34M	2.19M	32580

- We observe almost 21 million attacks over 2 years
  - Targeting 6.34M unique IPv4 addresses
  - average of 30k daily
- 2.19 million /24s had at least one IP address targeted
  - This number is about a third of recent estimates of the actively used IPv4 address space

Blackholing

- An IMC 2017 paper from CAIDA looks at BGP Blackoling[1]
  - Presents a methodology to infer BH events
    - Using RV, RIS &private BGP data sets, ...
    - Natural language processing to get BH communities
  - And, among others, characterizes BH practices and efficacy

- BH can be used for, e.g., DoS attack mitigation (and censorship)

[1] V. Giotsas et al., Inferring BGP Blackholing Activity in the Internet. In IMC’17.

A gap to be filled

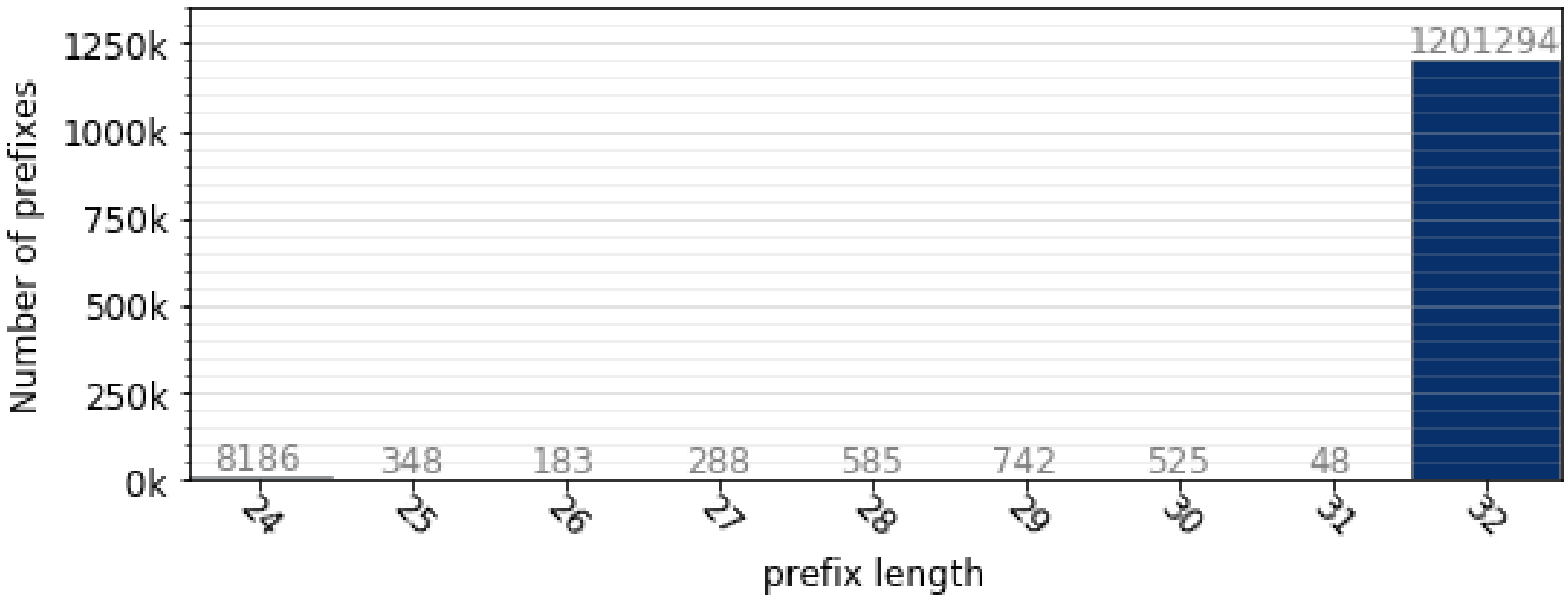
- A large-scale analysis of *Who blackholing affects* is missing
  - Active DNS measurement data gives us:
    - Web sites
    - DNS infrastructure (i.e., NS records)
    - And mail infrastructure (i.e., MX records)
- In addition, a correlation with DoS attacks is missing
  - We have darknet-inferred attacks & amplification honeypot logs

What are we doing?

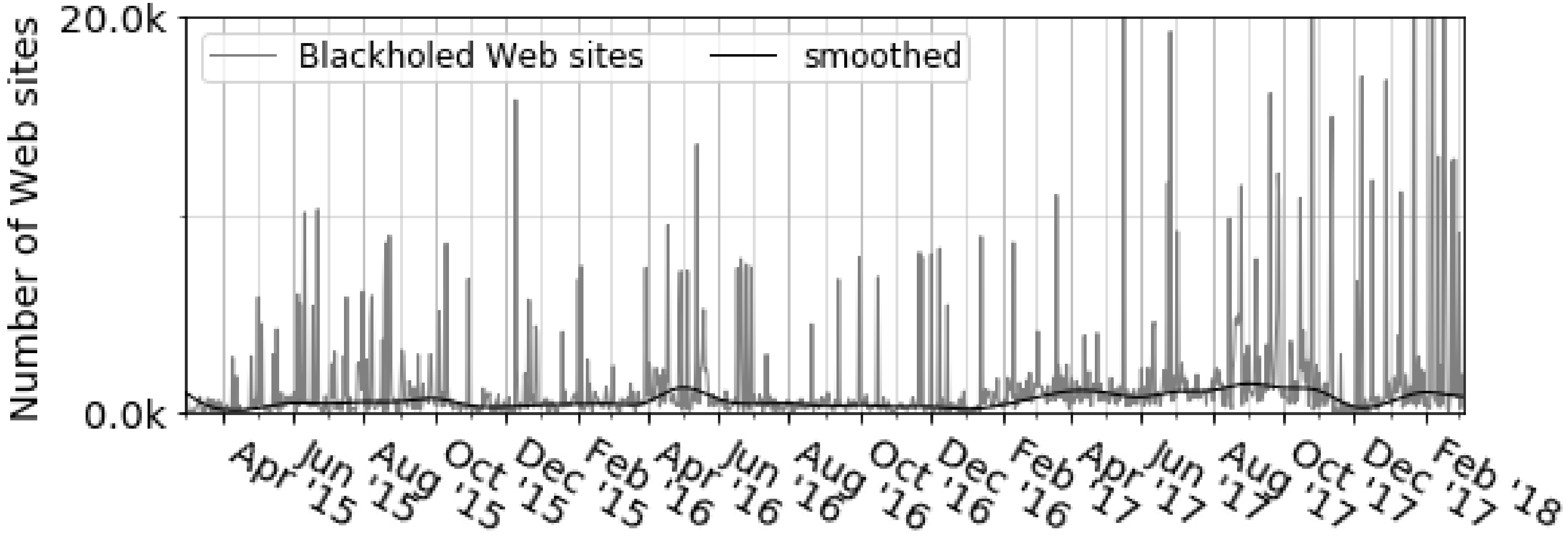
- Studying 1100 days worth of data (March 1, '15 – March 5, '18)
  - DNS measurement data (e.g., .com, .net, .org, alexa)
  - DoS attack events (ucsd-nt, amppot)
  - Blackholing events (using PyBGPStream in live mode to observe BH communities)
- Actively triggering traceroutes to BH'd /32s using RIPE Atlas
  - Ideally from 3 {peer,provider,customer} probes (determined using CAIDA's ASRank)
  - And to a second IP (using the USC/ISI IPHitlist)
  - Upon "activation" and "deactivation"

A peak at some results

- ~1.35 million BH events for 1100 days
- ~15% are preceded by attacks in the ucsd-nt data



Web site associations

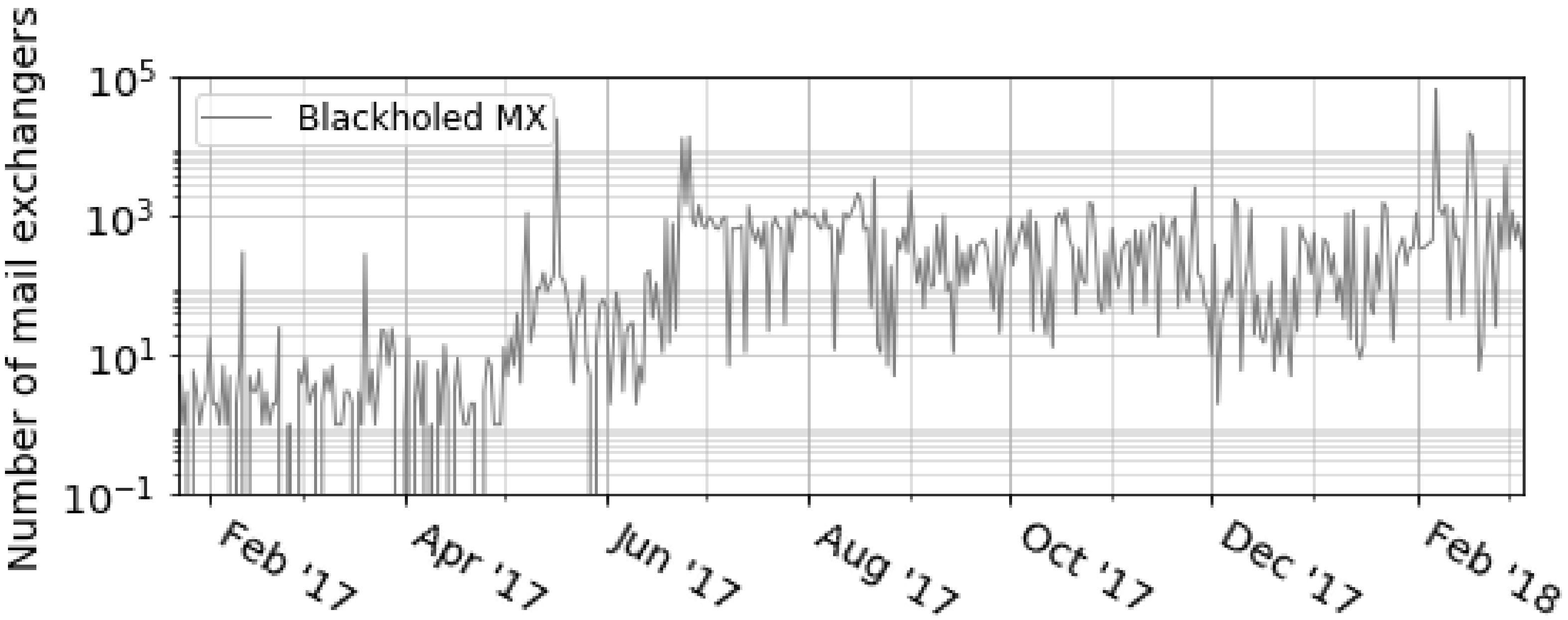


mean=1.6k; max=110k

n.b.:

- Inferred based on the presence of a www. label
- TODO: investigate redundant hosting

Mail server associations

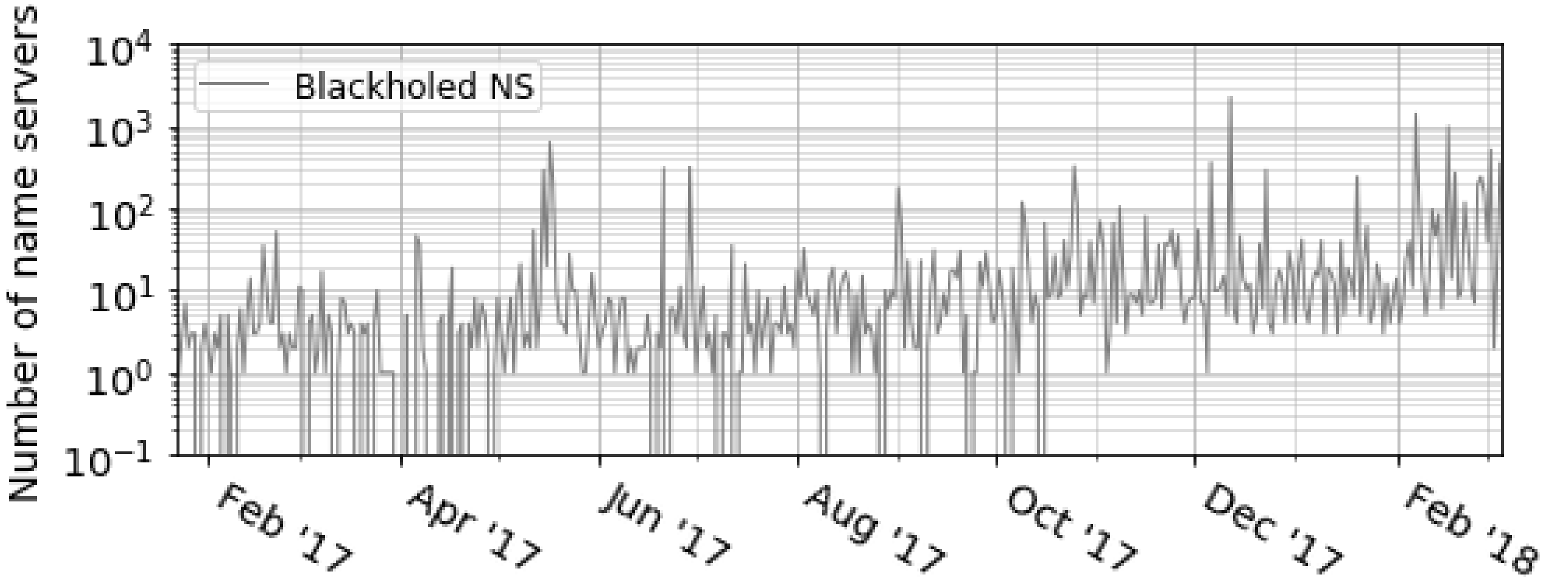


mean=709; max=~67.5k

n.b.:

- Inferred based on MX records

Authoritative name server associations

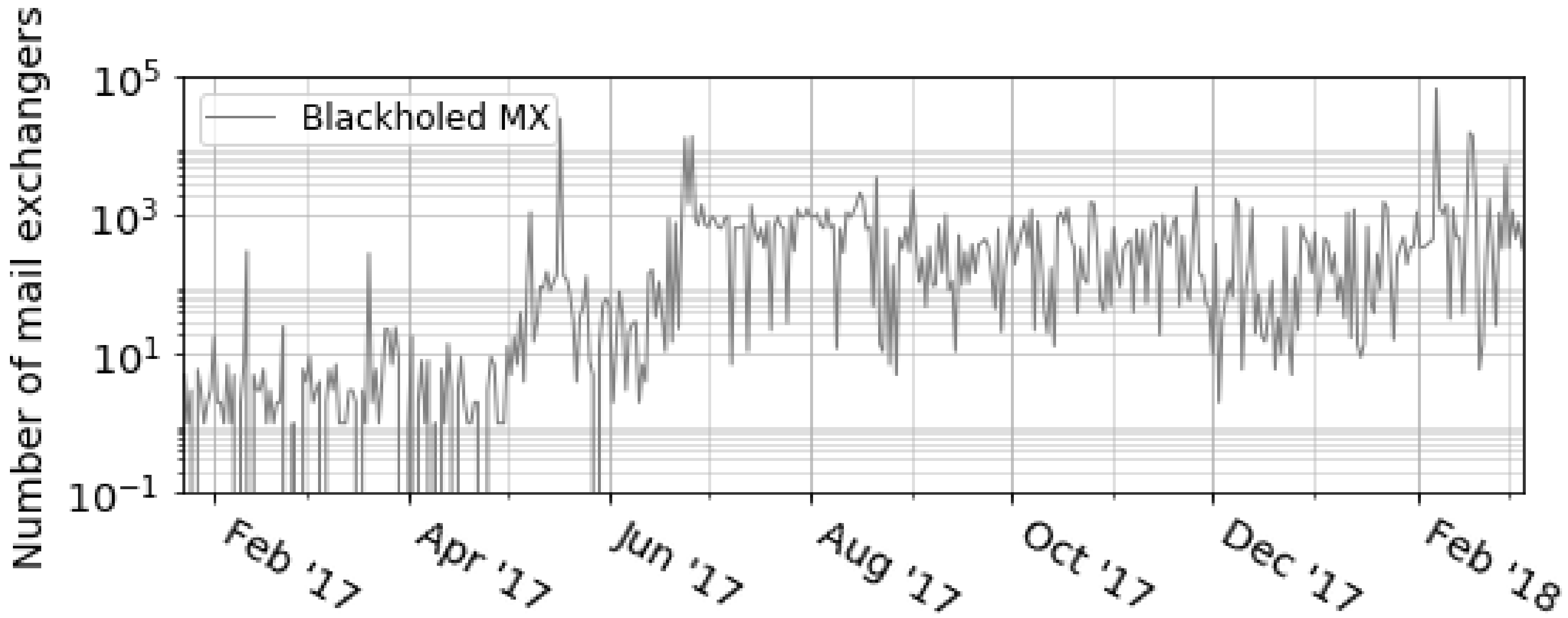


mean=~34; max=2224

n.b.:

- Inferred based on NS records

Mail server associations



mean=1.6k; max=110k

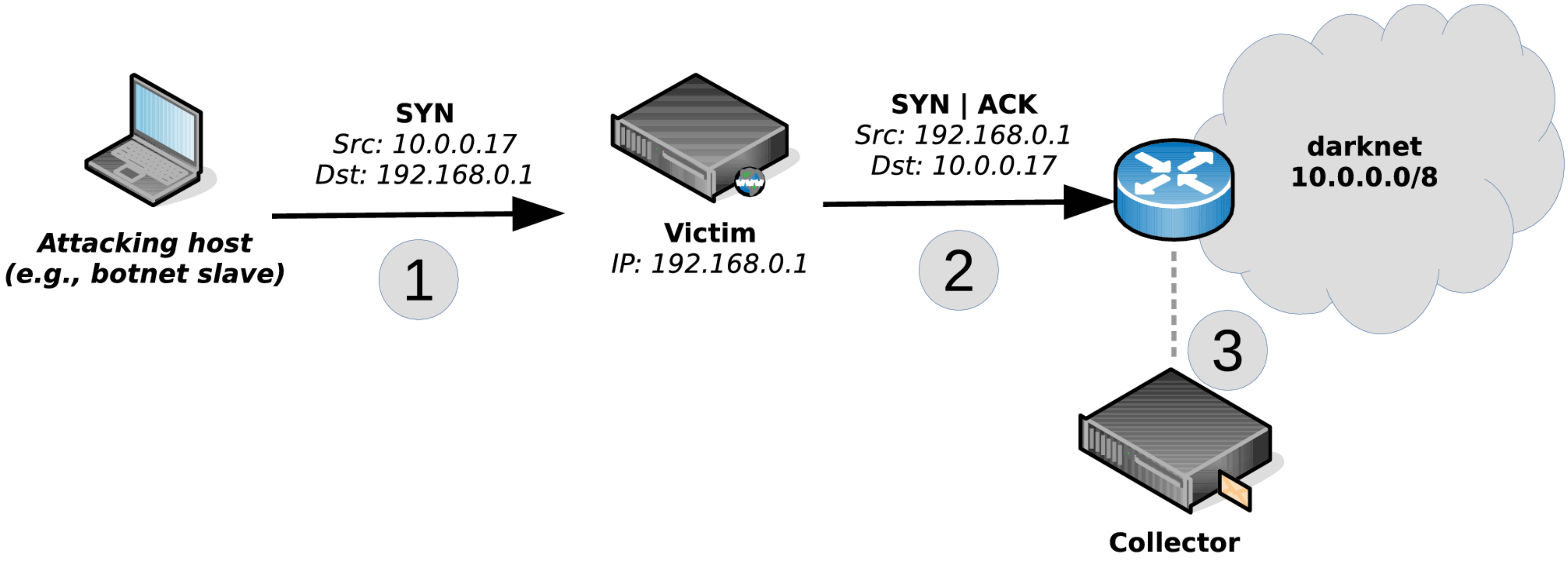
n.b.:

- Inferred based on MX records

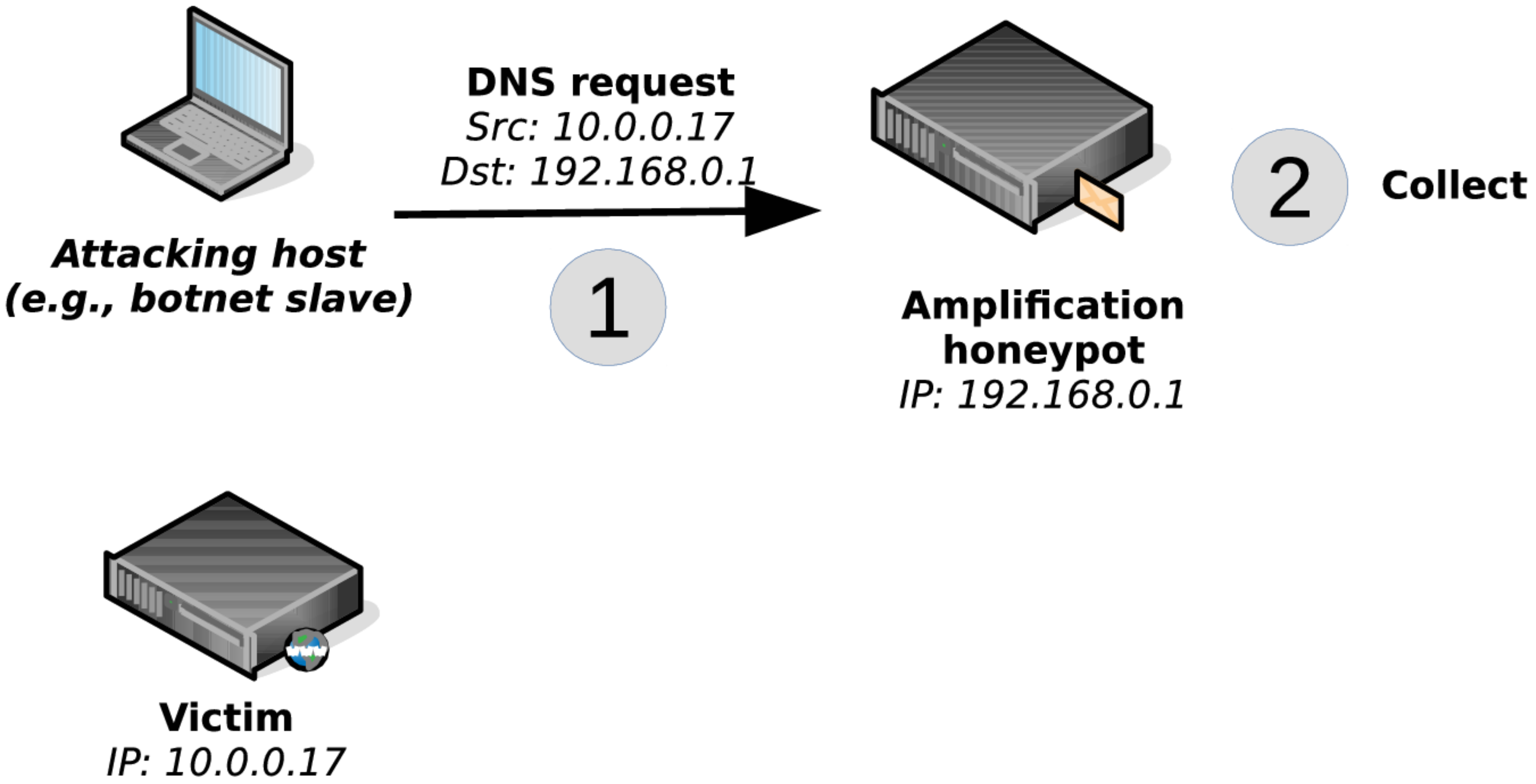
Questions?

Mattijs Jonker
m.jonker@utwente.nl

UCSD Network Telescope



Amplification honeypot (AmpPot)


DNS request
Src: 10.0.0.17
Dst: 192.168.0.1
Attacking host
(e.g., botnet slave)
1
Amplification
honeypot
IP: 192.168.0.1
2
Collect
Victim
IP: 10.0.0.17