SIDN Labs
Projects & Collaboration

Elmer Lastdrager | CENTR R&D Leiden

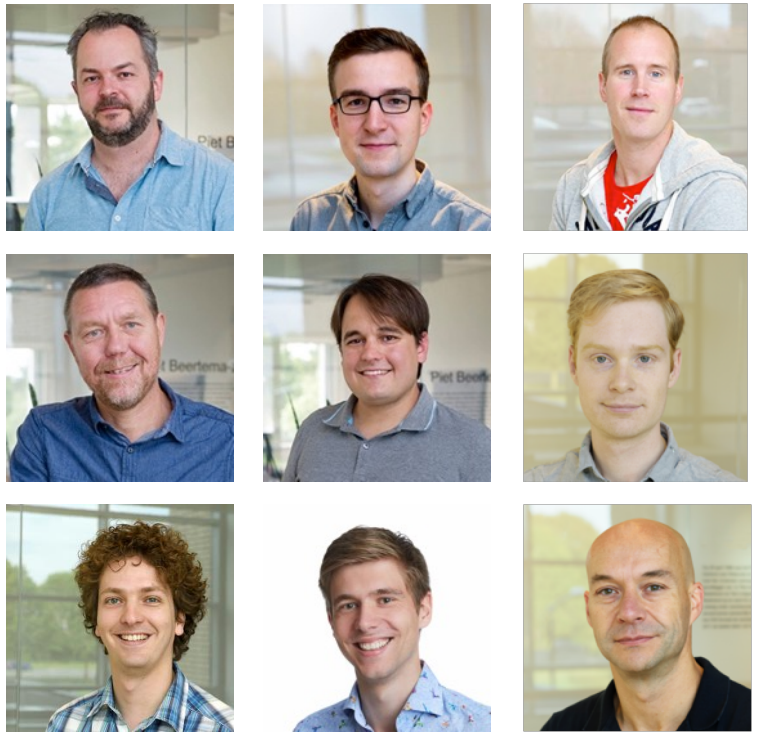
27-28 November 2018

SIDN Labs = research team

- Goal: advance operational security and resilience of end-to-end Internet comms through world-class measurement-based research and technology development

- Challenges: DNS resilience and security, domain name abuse mitigation, IoT security, collaborative security, Internet evolution, AAA infrastructures (new)

- Daily work: help operational teams, write open source software, analyze vast amounts of data, run experiments, write academic papers, work with universities



When the Dike Breaks: Dissecting DNS Defenses During DDoS

Part 1: (a) define user experiences; and (b) evaluate caching

Register .nl domain, two unicast NS, Ripe Atlas as vantage point
Each probe unique query, every 20 minutes, variable TTL.
->70% caching works, 30% of clients caching not effective.

Part 2: verify results of part 1 in production zones (.nl)
experiment works like in real zone

Part 3: emulate DDoS in the wild to observe user experiences
Simulate packetloss (50%, 90%, 100%)
50%: Nearly all clients get an answer.
90%: Most clients (60%) get an answer, eventually.

100%: 35-75% of clients served from cache

SIDN LABS

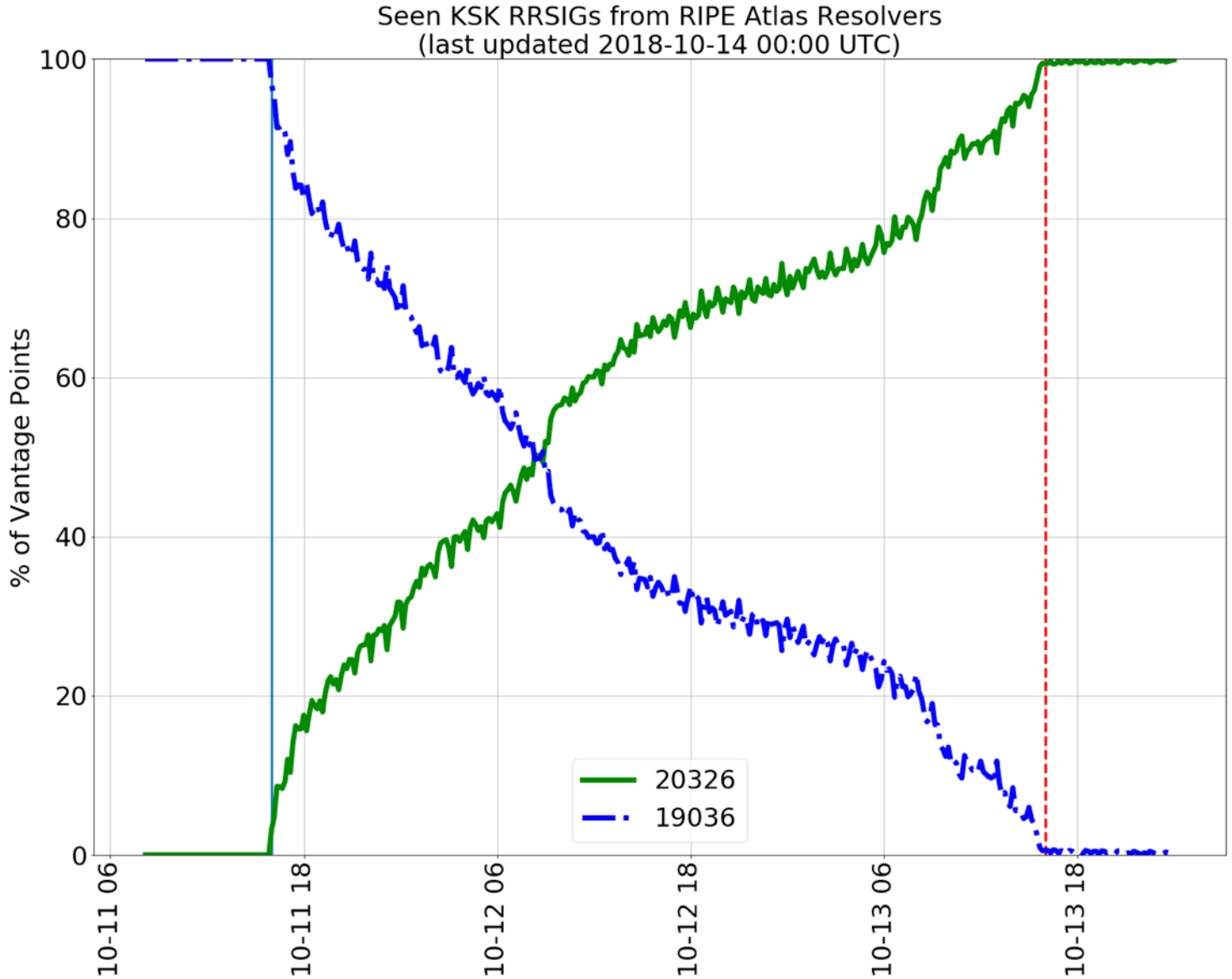
When the Dike Breaks: Dissecting DNS Defenses During DDoS

Giovane C. M. Moura, John Heidemann, Moritz Müller, Ricardo de O. Schmidt, and Marco Davids.. **When the Dike Breaks: Dissecting DNS Defenses During DDoS**. In Proceedings of the Internet Measurement Conference 2018 (IMC '18). ACM, New York, NY, USA.

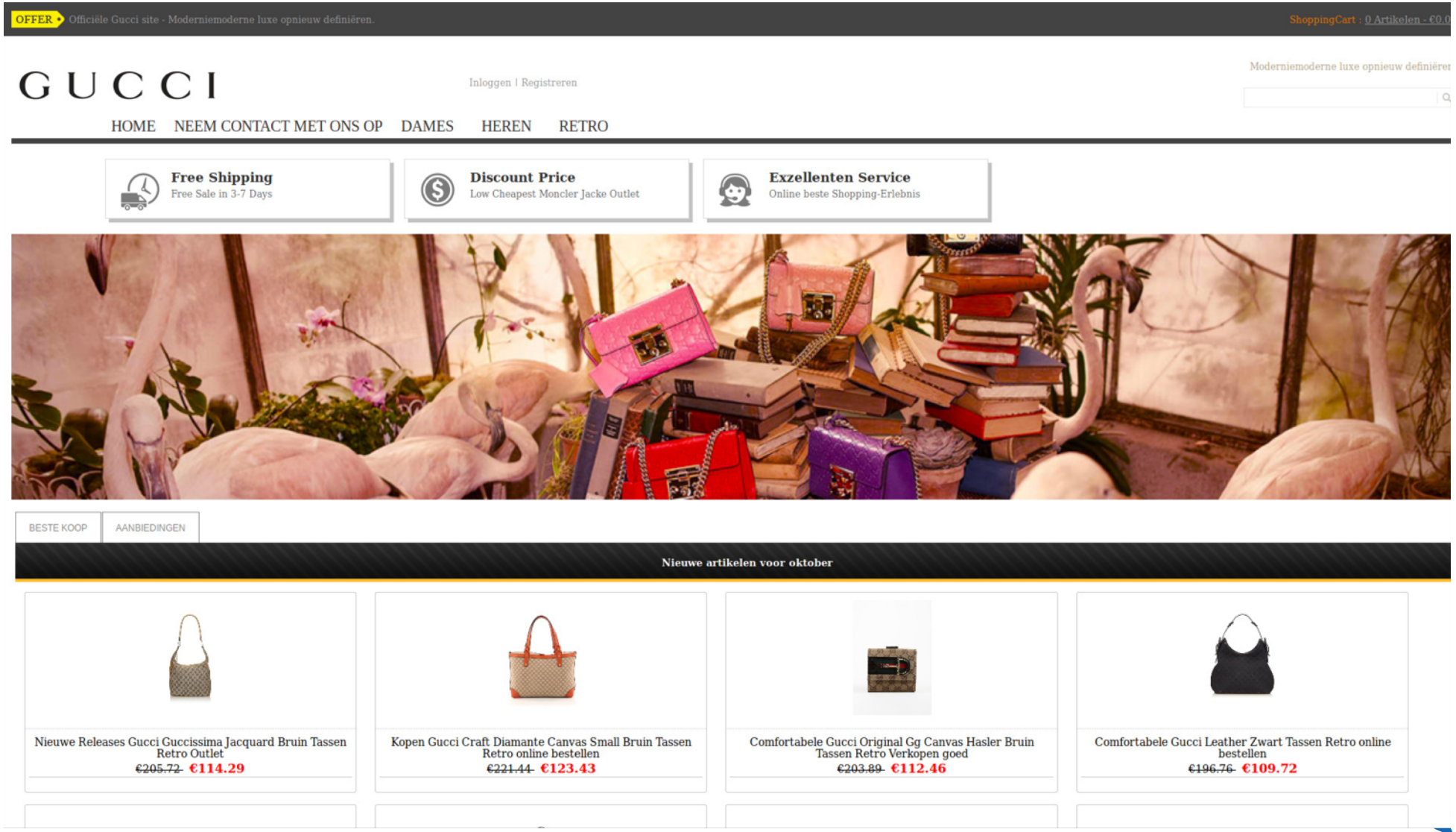
Download from https://www.sidnlabs.nl

SIDN LABS

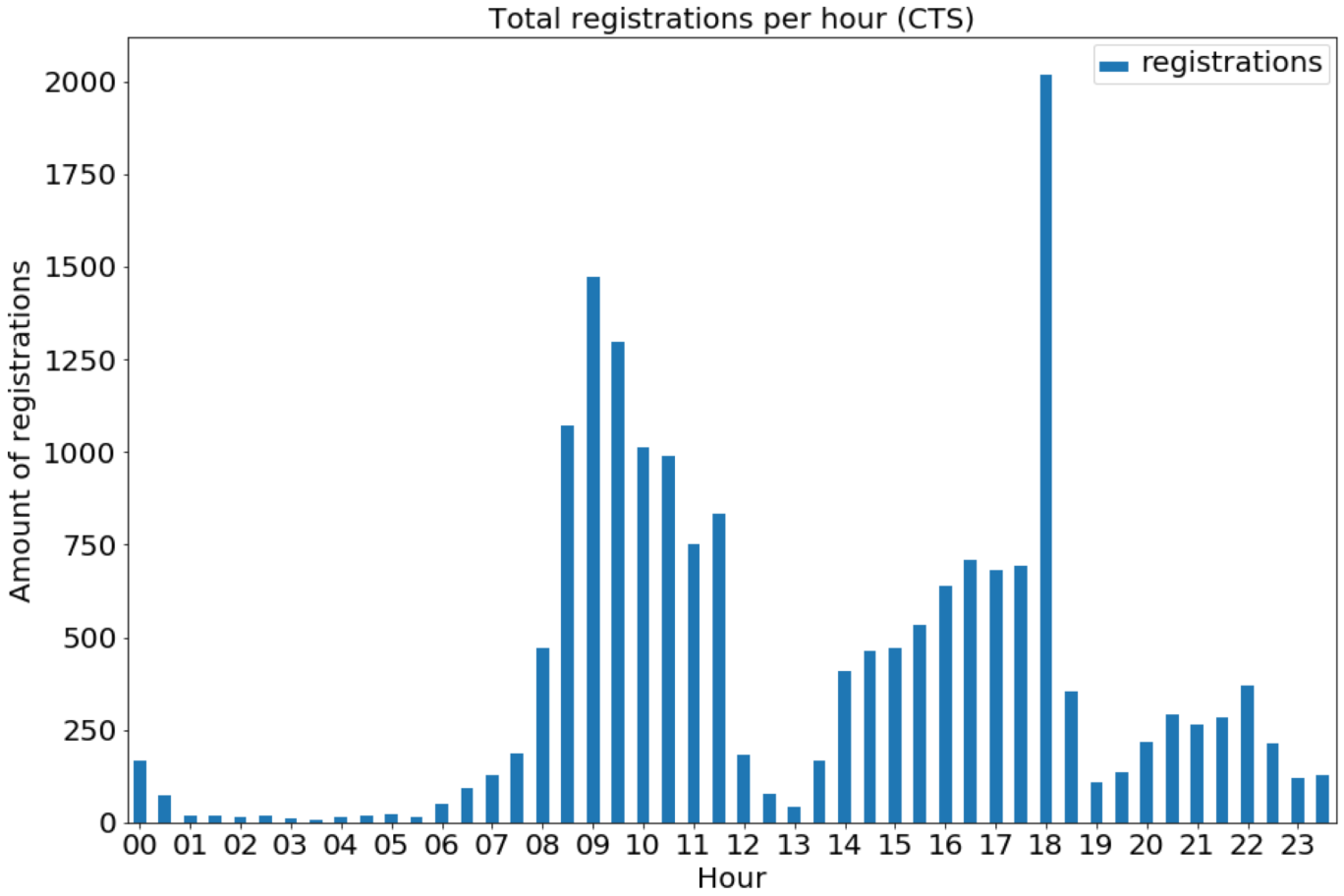
KSK rollover monitoring



Fake webshops



Fake webshops: registration times



Detecting botnets in DNS data

MINIONS

DAGOBERT

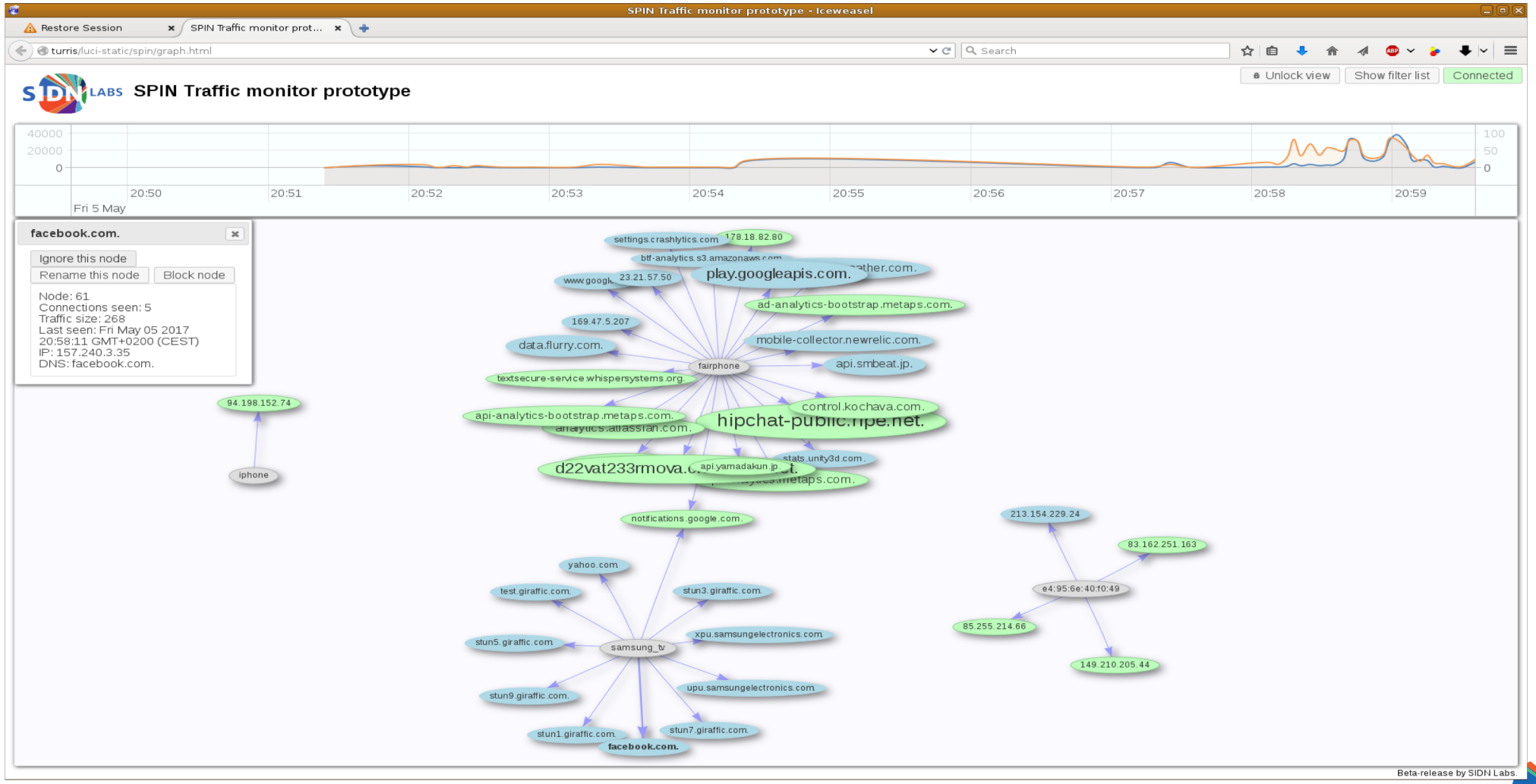
Looking at ISP-resolver data, use .nl nameservers data (ENTRADA).

SPIN (IoT Security)

- Security and Privacy for In-home Networks
- Research and prototype SPIN functions:
  - Visualize network traffic
  - Automatically block unwanted traffic/infected devices
  - Allow ‘good’ traffic
  - Sharing platform for device info
- Open source in-home router/AP software that
  - Helps end-users control their security and privacy in the IoT
  - Helps protecting DNS operators (like SIDN!) and other service provides from IoT-powered DDoS attacks
  - All processing done locally, no VPN, no enforced cloud

SIDN LABS

SPIN (IoT Security)



SPIN (IoT Security)

Current topics of interested (high level):

- (Local) measurements on devices
  - Privacy
- Anomaly detection
  - What is normal behaviour?
  - What is ‘different’ behaviour?
  - How to tell if it’s bad? (Hacked vs, say, yearly software update)

SPIN (IoT Security)

Current topics of interested (high level, continued):

- Collaboration on security information, such as vetted MUD profiles (Manufacturer usage description)
  - Manufacturer Usage Description (IETF draft, started by Cisco)
  - Specifies which names, ports, and addresses are used
  - Firewalls can open up only those ports
  - Will manufacturer implement it?
- Network subdivision
  - Divide classes of devices into their own subnet
  - What about Sonos/Airplay/etc.?

SDN LABS

Other projects

Concordia (EU-funded): DDoS clearing house

Future internet (see presentation Caspar)

Collaboration

For example:

- MUD profiles (making, evaluating, sharing)
- Sharing traffic traces of IoT devices
- Homenet topology measurements
- …

Thanks for your attention!

SDN LABS