

Security and Privacy for In-home Networks

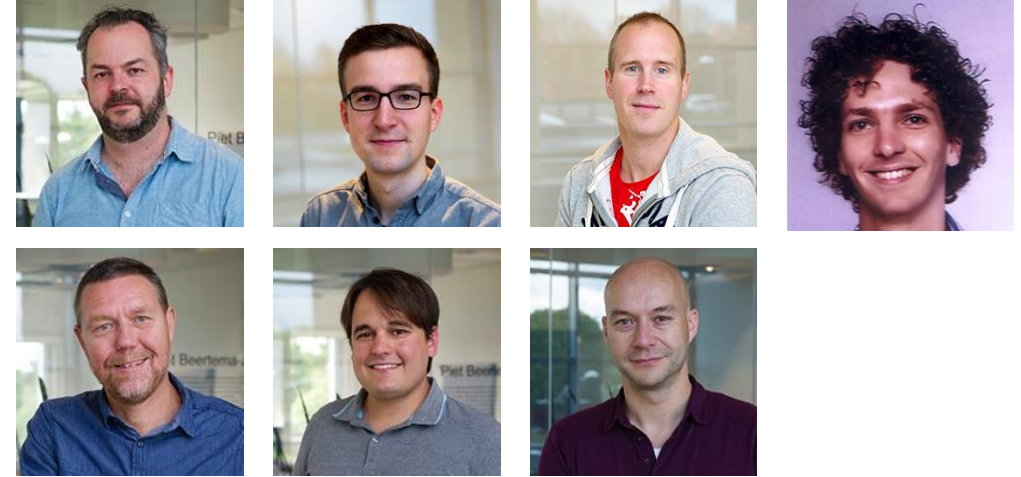
Jelte Jansen | Holland strikes back

3 oktober 2017



SIDN Labs

- Research team of .nl registry, SIDN
- Goal: thrust operational security, resilience, and privacy of the Internet through world-class measurement-based research and technology development
- Themes: DNS service management, topology mapping & anomaly detection, IoT homenet management
- Targeted impact: SIDN, .nl ecosystem, wider Internet community



.nl = the Netherlands
17M inhabitants
5.7M domain names
2.6M DNSSEC-signed
1.3B DNS queries/day



8.4 Billion

Devices connected to the Internet in 2017

Source: Gartner (January 2017)

20 Billion
in 2020



The "S" in IoT
stands for
SECURITY



Attributed to @tkadlec



The 2016 Dyn attack

Mirai

vs.



DynSM

1.2 Tbps

From 'only' 100.000 devices

What can we do?

For various interpretations of 'we'



What should we do?

- Better practices for manufacturers?
- Free **secure** software stacks?
- International policy, regulation, certification?
- Clear up accountability issues?
- Generate market demand for secure products?
- Quarantine bad actors (e.g. at ISP)?
- Educate users?
- Empower users?

“Yes”

We need to do it all

For various interpretations of ‘we’



Focus on one today:

Empower users:

Protect home networks

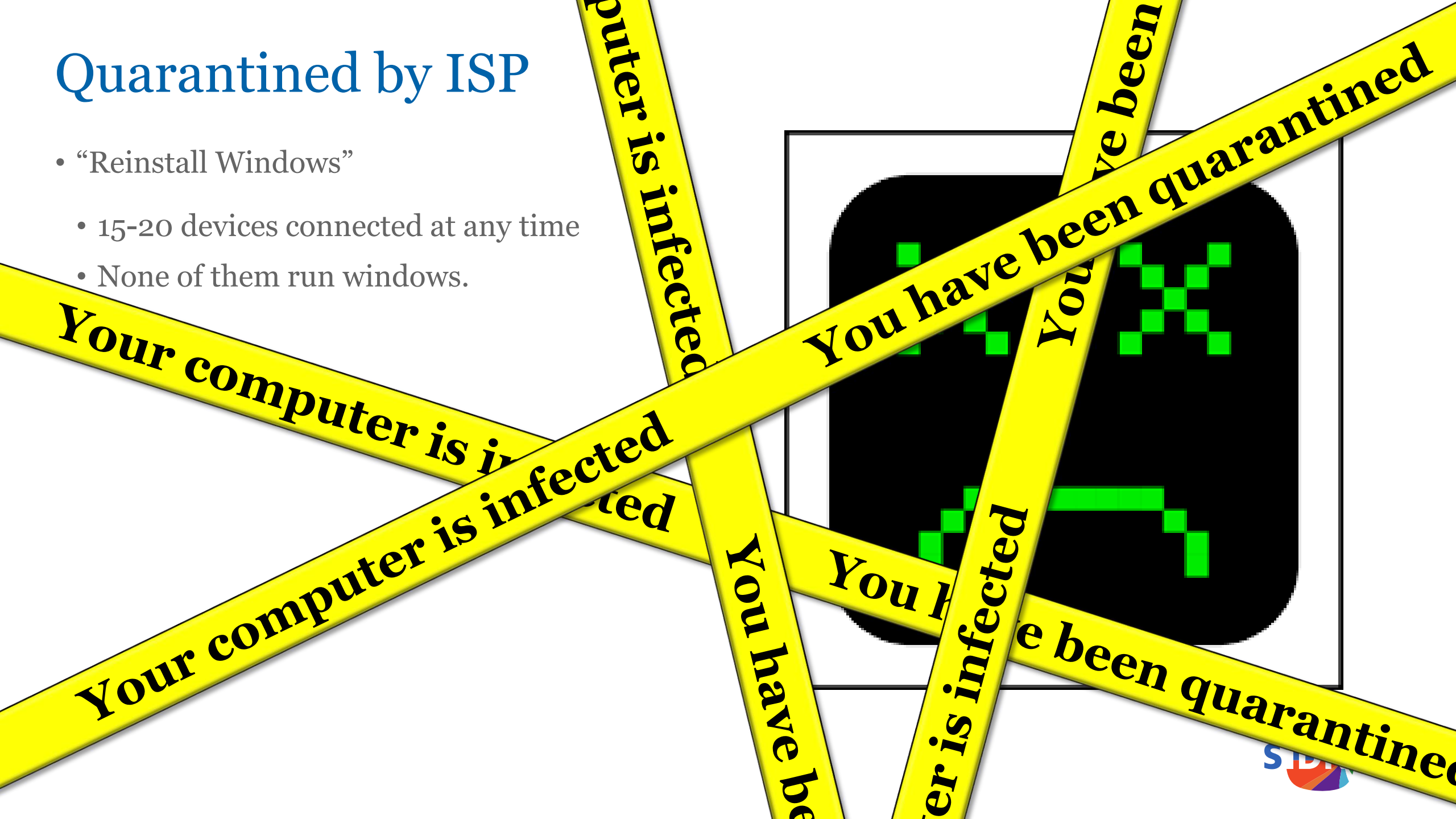
How to protect home networks?

- Home networks notoriously insecure
- Many different devices and device types
- There will always be bad devices and computers



Quarantined by ISP

- “Reinstall Windows”
- 15-20 devices connected at any time
- None of them run windows.



How to protect home networks?

- Lowest common denominator: IP
- So, firewall?
- We need something better

```
jelte@dragon: /home/jelte
wired = "em1"
wifi = "athn0"
table <martians> { 0.0.0.0/8 10.0.0.0/8 127.0.0.0/8 169.254.0.0/16 \
                  172.16.0.0/12 192.0.0.0/24 192.0.2.0/24 224.0.0.0/3 \
                  192.168.0.0/16 198.18.0.0/15 198.51.100.0/24 \
                  203.0.113.0/24 }

set block-policy drop
set loginterface egress
set skip on lo0
match in all scrub (no-df random-id max-mss 1440)
match out on egress inet from !(egress:network) to any nat-to (egress:0)
antispoof quick for { egress $wired $wifi }
block in quick on egress from <martians> to any
block return out quick on egress from any to <martians>
block all
pass out quick inet
pass in on { $wired $wifi } inet
pass in on egress inet proto tcp from any to (egress) port { 80 443 } rdr-to 192.168.1.2

1,1 All
```

The Dream

A surreal landscape with a girl in a blue dress looking at a whale carrying a castle on its back, flying over a sea of clouds. The scene is set against a backdrop of a sunset or sunrise sky, with a forest of evergreen trees visible on the left side of the image.

Open home security platform: open source, open standards

Automatic operation: guards and automatically blocks devices

Privacy friendly: runs locally, does not process application-level data

User-centric: automatic, but allow for 'power-use'

Enables new business models: network-level system w/ well-defined APIs

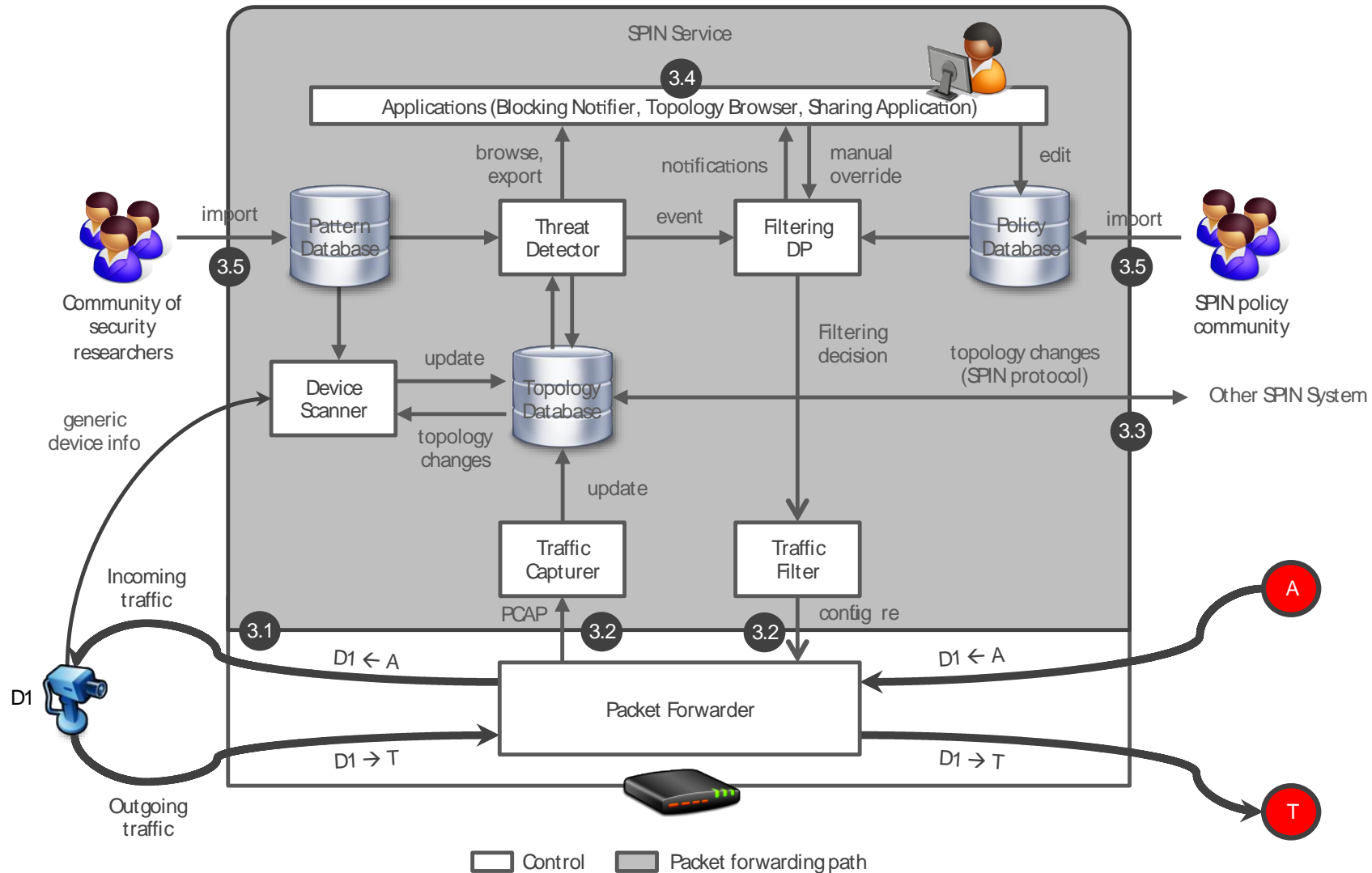
The SPIN project at SIDN Labs

- Open source in-home router/AP software that
 - Helps end-users control their security and privacy in the IoT
 - Helps protecting DNS operators and other service providers from IoT-powered DDoS attacks
 - All processing done locally, no VPN, no cloud

The SPIN project at SIDN Labs

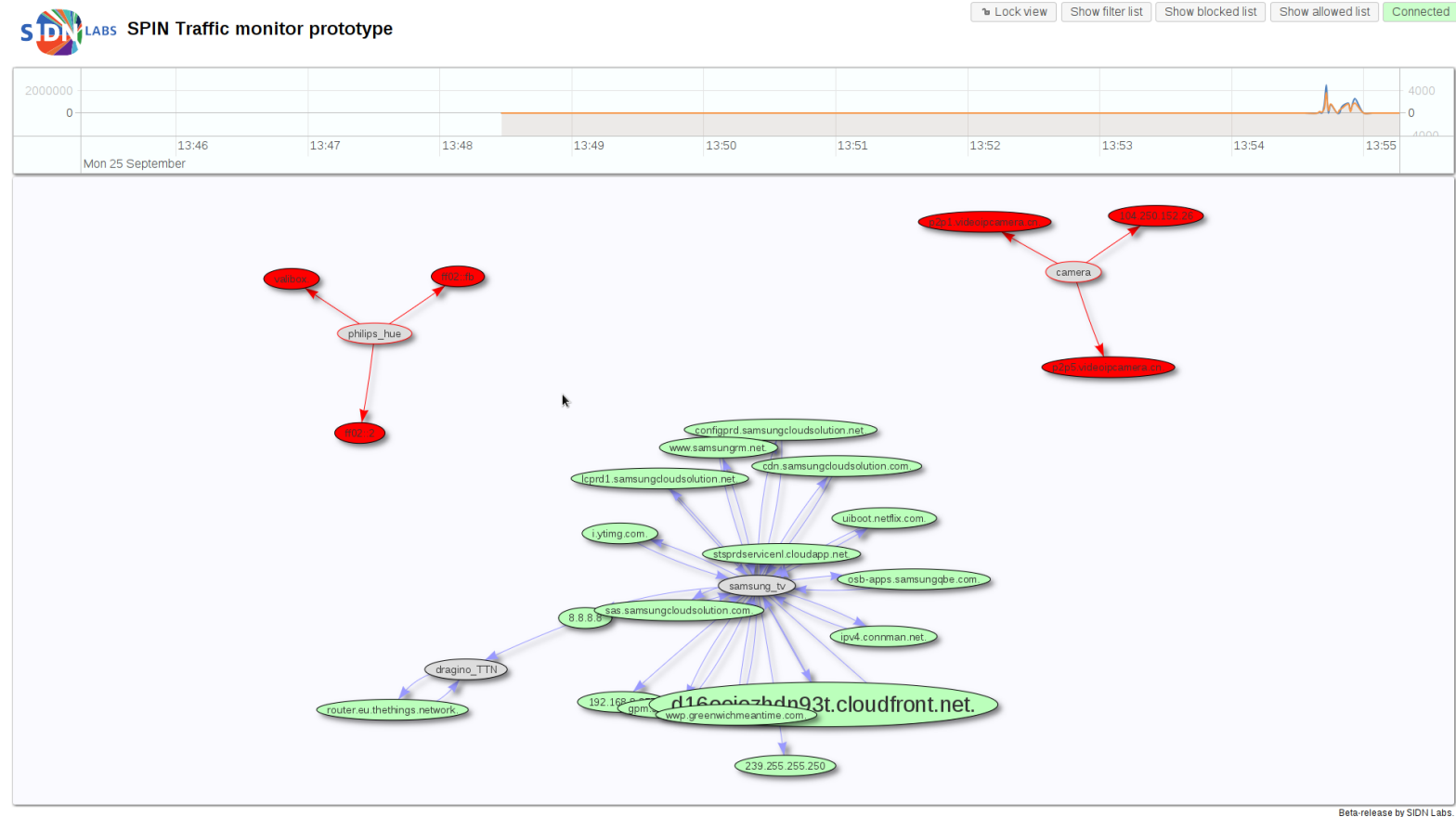
- Research and prototype SPIN functions:
 - Visualise network traffic
 - Automatically block unwanted traffic/infected devices
 - Allow 'good' traffic
 - Scan devices
 - Sharing platform for device info

High-level view



Status

- Running prototype
- ‘Vertical slice’ of the concept
- Visualises basic traffic
- Blocks specified traffic



- Open source: <https://github.com/SIDN/SPIN>
- Full (GL-Inet) images at <https://valibox.sidnlabs.nl/>

Future Research

- This needs to be a collaborative effort
- Collaborate on experiment visualisation/control
- Collaborate on a platform for sharing (IoT) device information
- Research into device scanning
- Research ‘circuit-breaker’ design (think power groups)
- Possibly: Repositories for known bad devices/versions
(This might be a bad thing™!)
- Possibly: Trusted traffic profiles
“My TV should stream the news and Netflix, but nothing else”

Current high-level topics of interest

- Standardization
- Pilot for large scale evaluation
- Business models based on SPIN platform
- SPIN as a platform for IoT research projects

Demo!

In 5 minutes at Toyoda room



Follow us

 SIDN.nl

 @SIDN

 SIDN

Thank you for your attention!

Any questions?