Security and Privacy for In-home Networks

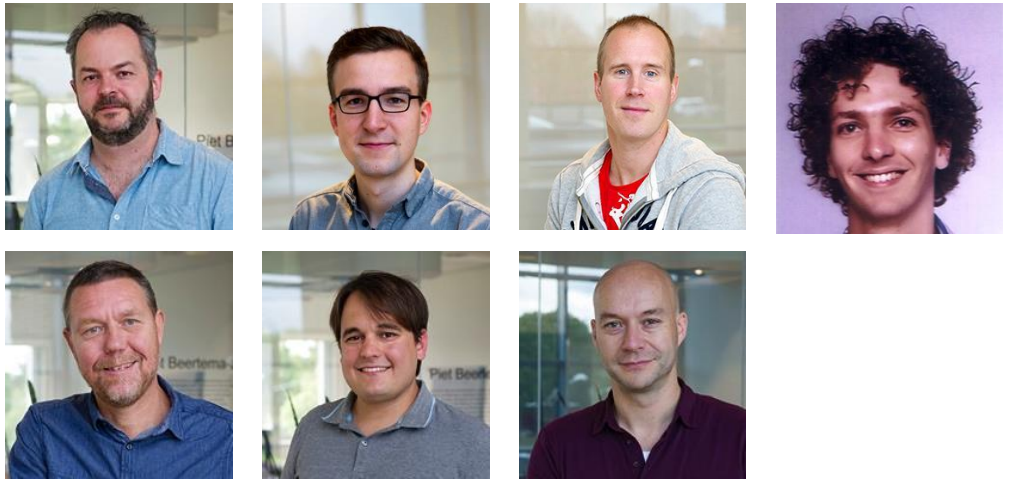
Jelte Jansen | Holland strikes back

3 oktober 2017

SIDN LABS

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

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

- Targeted impact: SIDN, .nl ecosystem, wider Internet community

8.4 Billion

Devices connected to the Internet in 2017

Source: Gartner (January 2017)

SDN LABS

20 Billion

in 2020

Attributed to @tkadlec

SDN LABS

The 2016 Dyn attack

Mirai vs. Dyn

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, certificiation?
- 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’

SIDN LABS

Focus on one today:

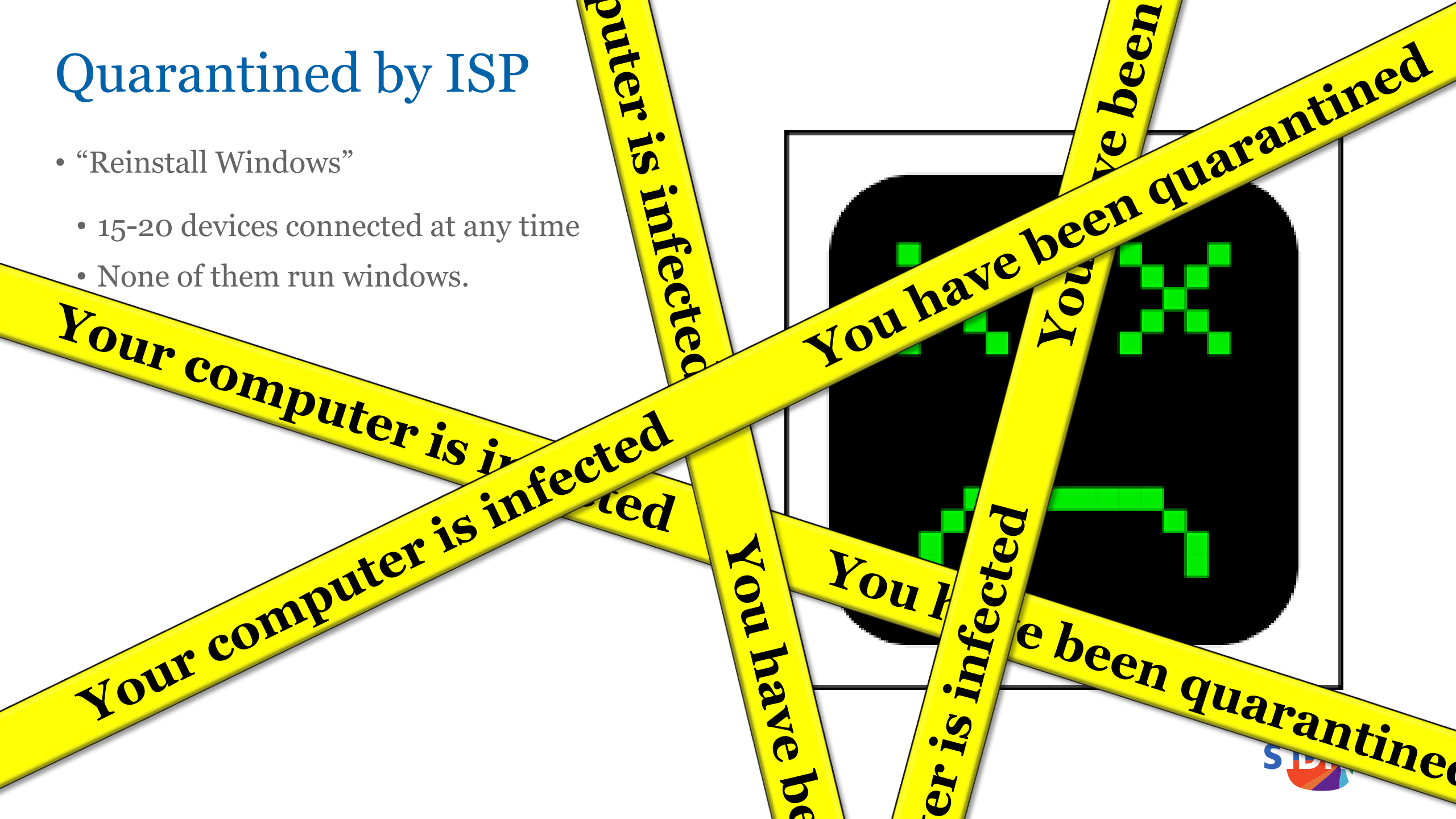
Empower users:
Protect home networks

How to protect home networks?

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

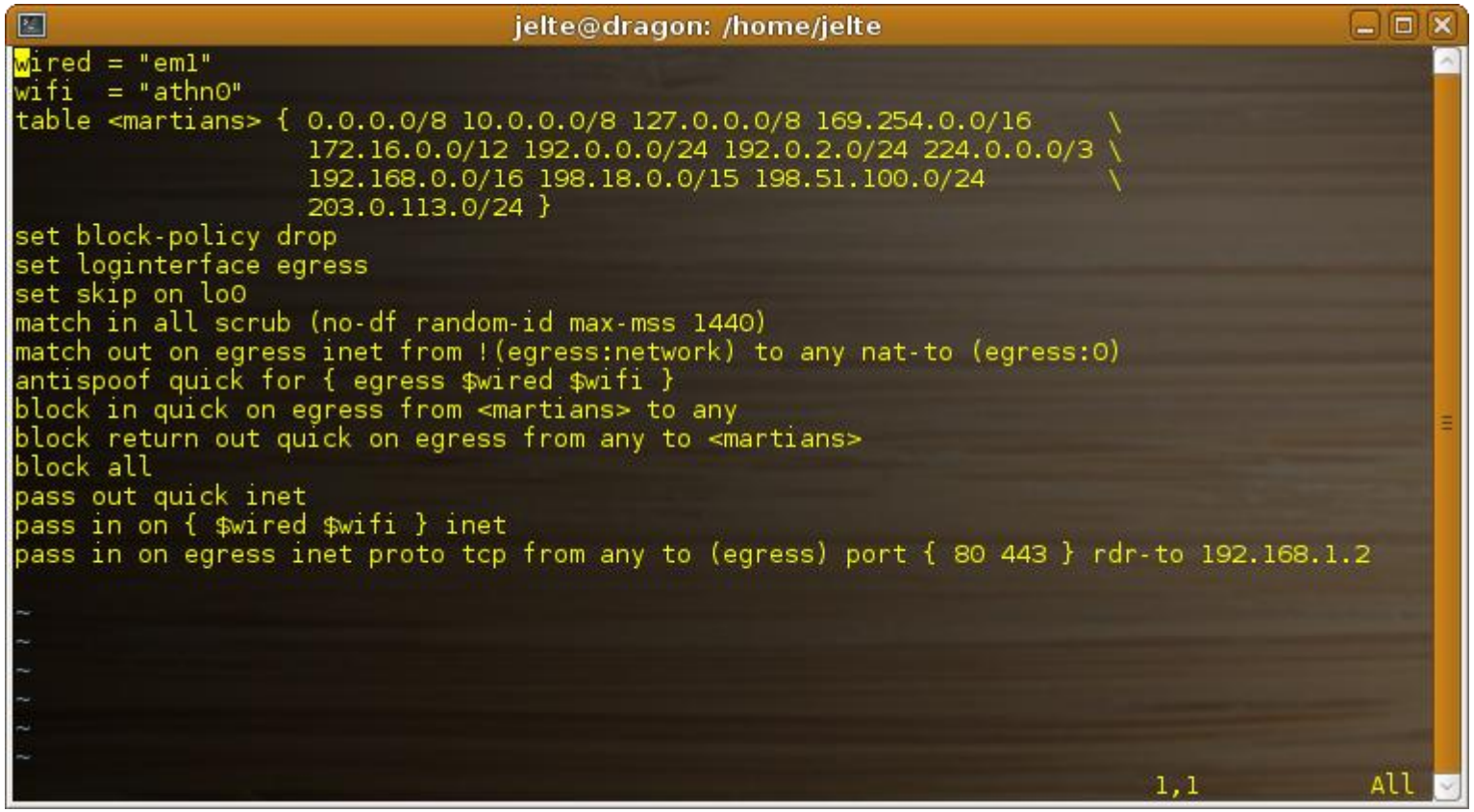
Quarantined by ISP

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

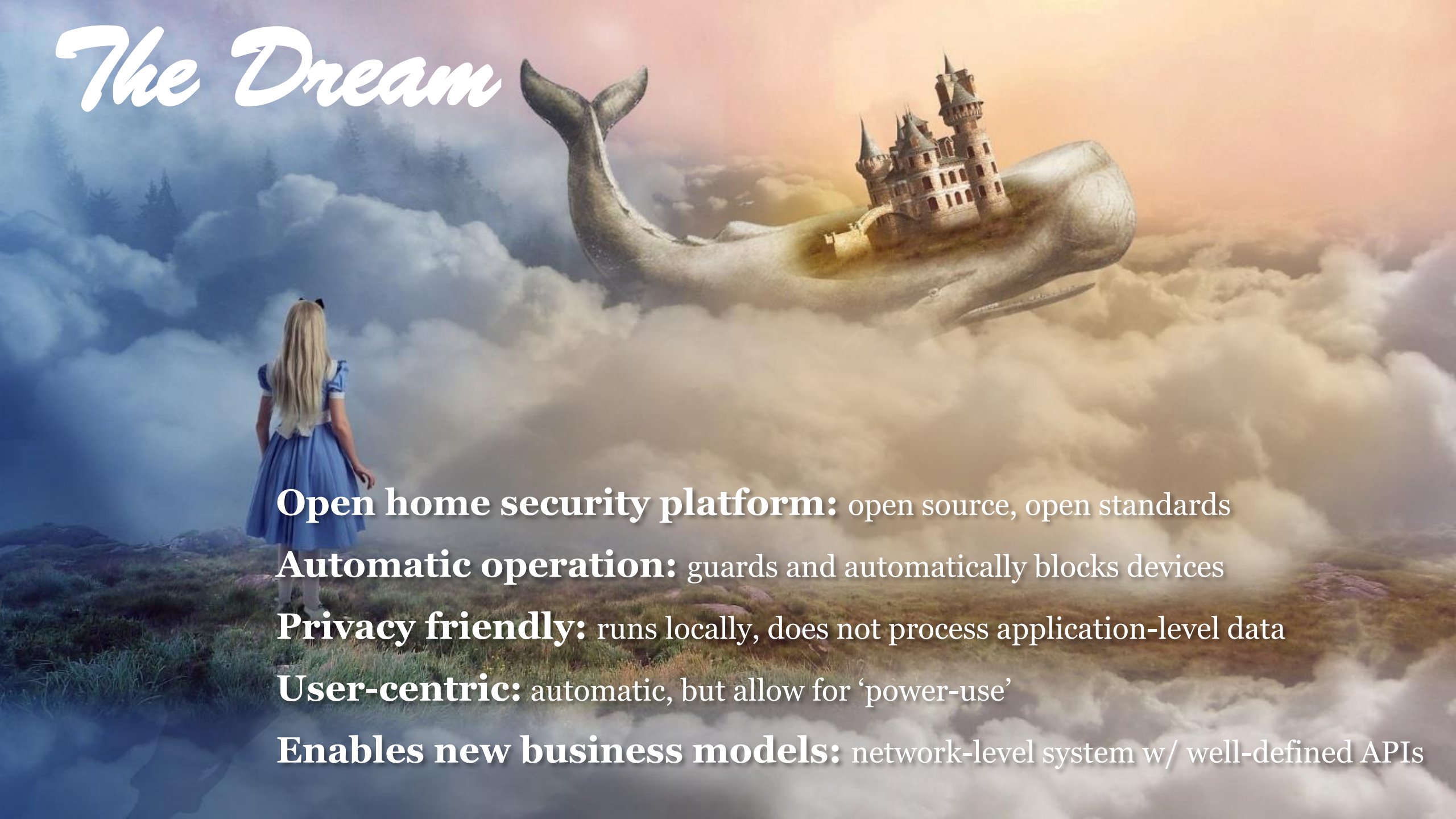


How to protect home networks?

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



The Dream



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

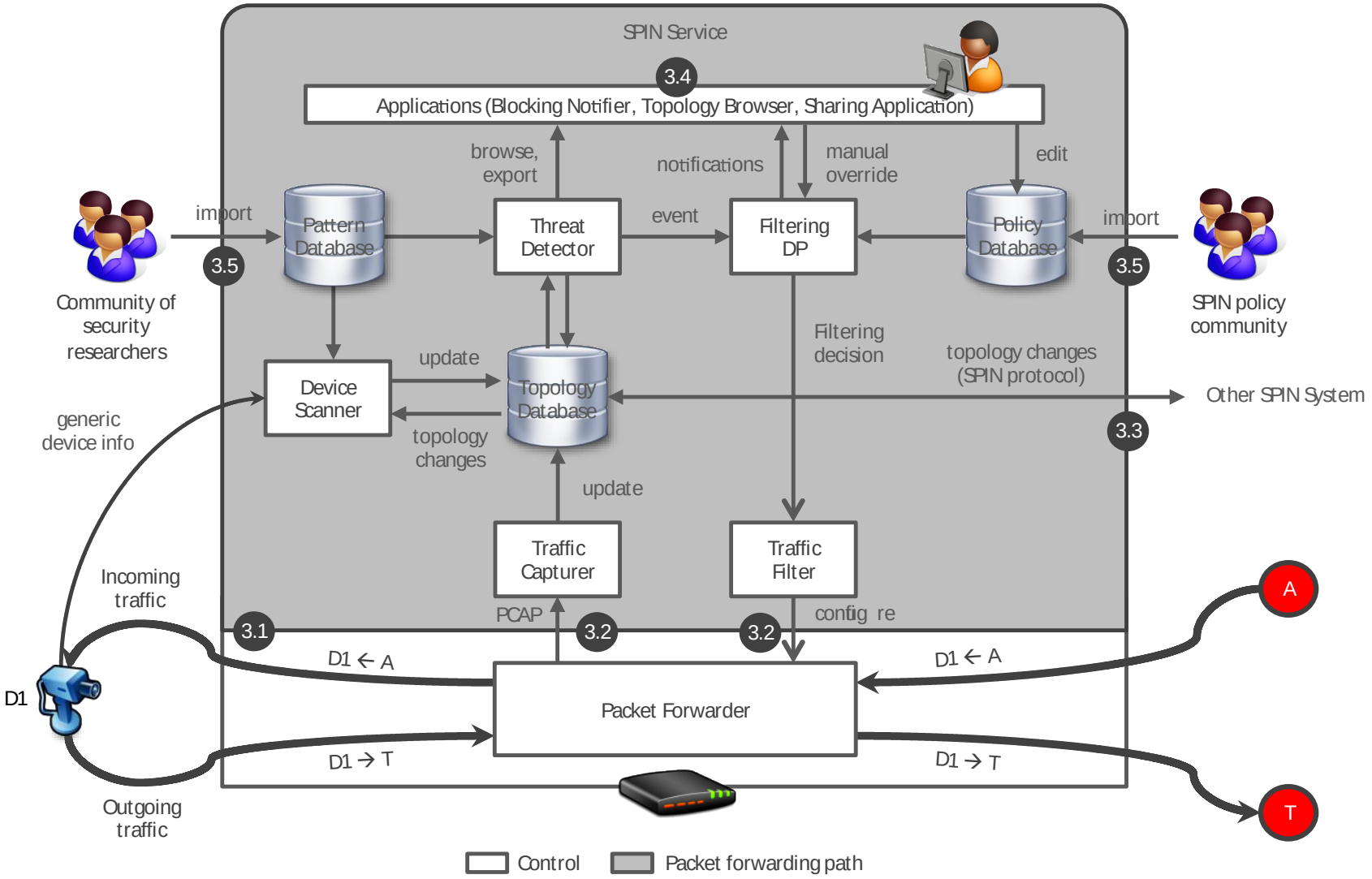
The SPIN project at SIDN Labs

- 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 provides from IoT-powered DDoS attacks
  - All processing done locally, no VPN, no cloud

The SPIN project at SIDN Labs

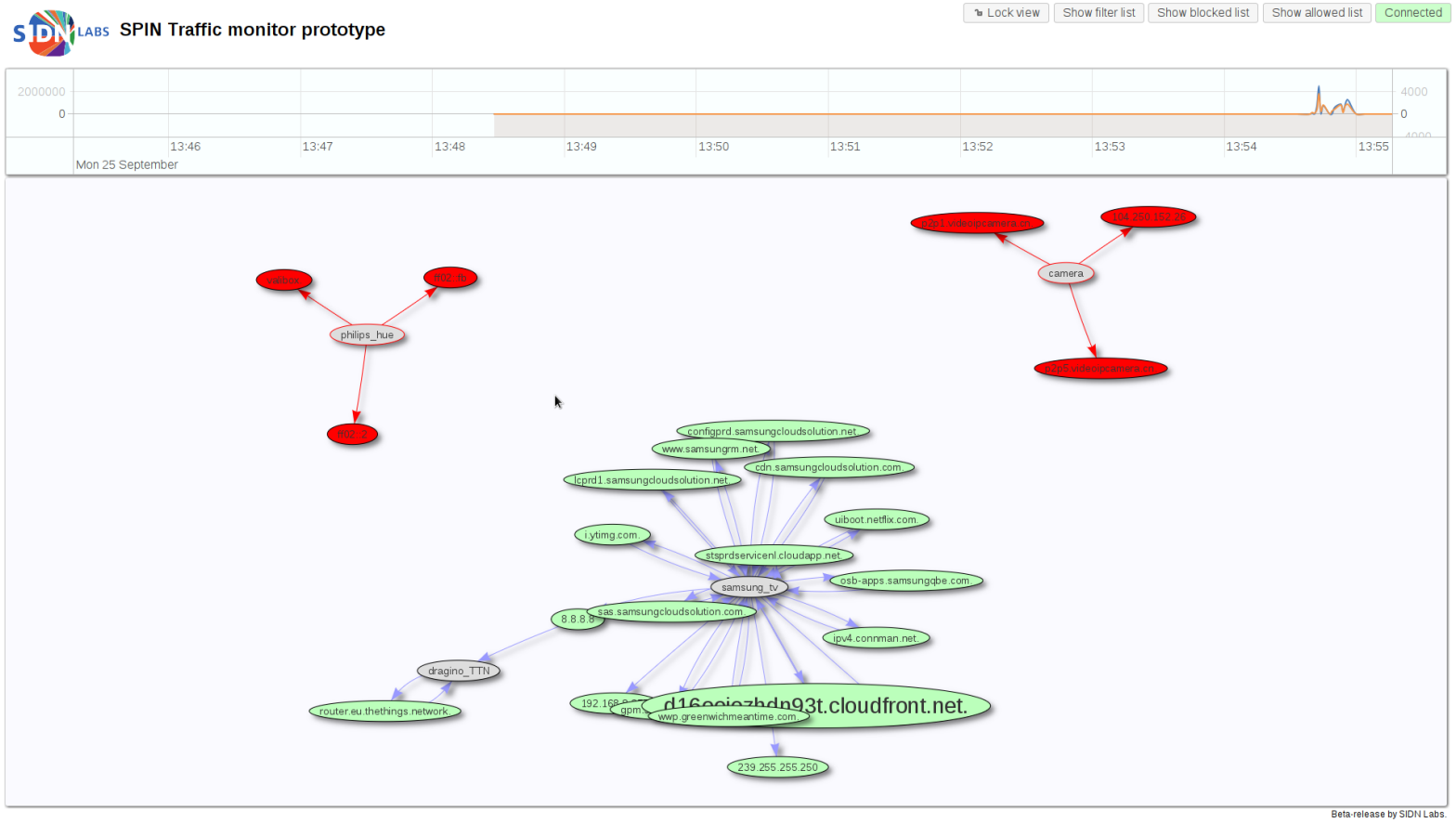
- Research and prototype SPIN functions:
  - Visualise network traffic
  - Automatically block unwanted traffic/infected devices
  - Allow ‘good’ traffic
  - Scan devices
  - Sharing platform for device info

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”

SIDN LABS

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

SIDN LABS

Demo!

In 5 minutes at Toyoda room

Follow us

SIDN.nl


@SIDN

SIDN

Thank you for your attention!

Any questions?

SIDN LABS