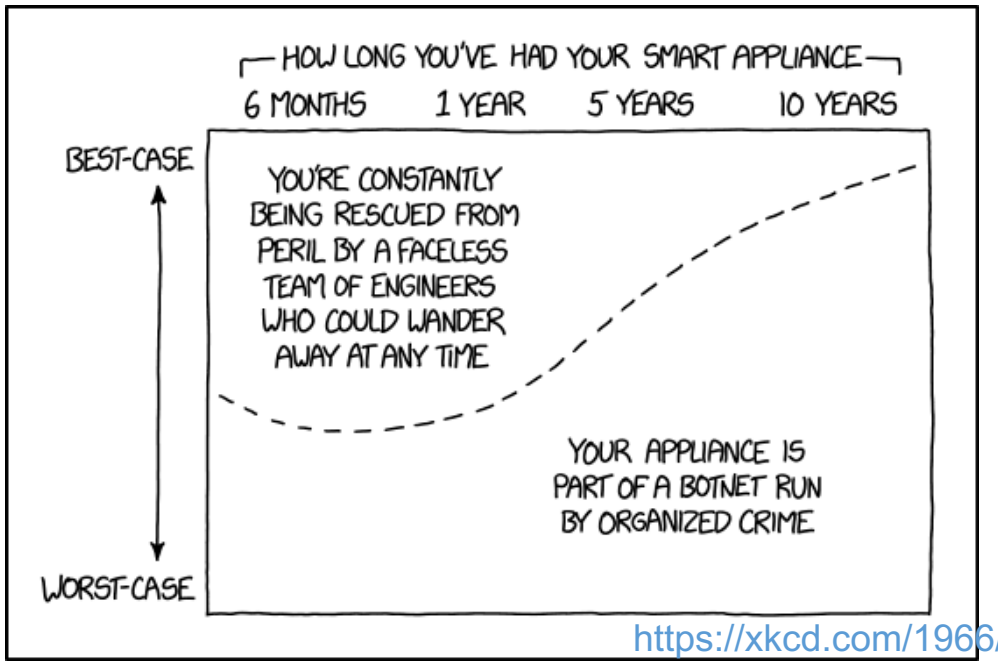
The Internet-of-Insecure-Things
Causes, Trends and Responses
(@ RIPE 77)



https://xkcd.com/1966/

Arman Noroozian

(Economics of Cybersecurity, TPM, @TU Delft, Netherlands)

Mirai: The IoT Bot That Took Down Krebs and Launched a Tbps DDoS Attack on OVH

Article security

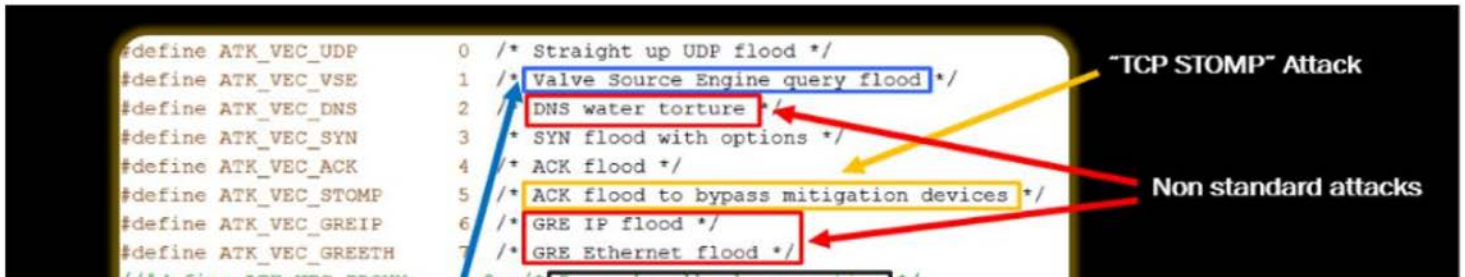
By **Liron Segal**

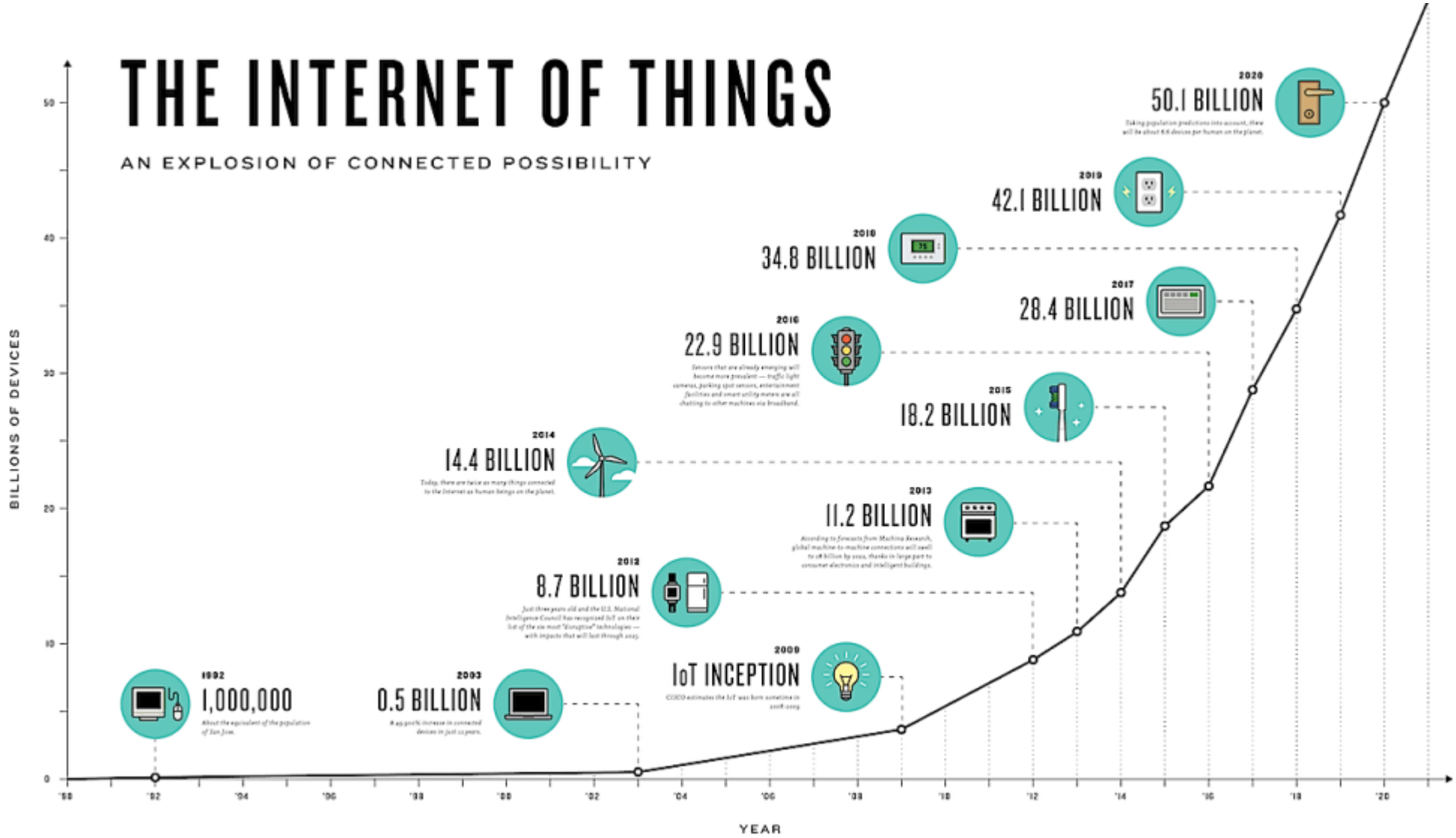
The "Mirai" botnet has infected hundreds of thousands of Internet of Things (IoT) devices, specifically security cameras, by using vendor default passwords for Telnet access. This IoT botnet successfully landed a Terabyte attack on OVH[1], and took down KrebsOnSecurity[2] with an Akamai-confirmed 620+ Gpbs attack. Following Mirai's author post, dissecting the malware's source code and analyzing its techniques (including DDoS attack methods that are rarely seen like DNS Water Torture and GRE) we can definitely expect the IoT DDoSing trend to rise massively in the global threat landscape.

IoT devices are very attractive to the DDoS business as they don't require additional expenses, social engineering attacks, email infection campaigns, exploit kits or fresh zero-days. It is common for these devices to have poor security standards such that their remote administration ports are publically accessible and susceptible to brute force and dictionary attacks, the ports are "protected" with vendor default passwords, and they don't have an anti-virus solution in place to prevent malware infections. Combine these gaping security holes that make them "easy to exploit," with the device managers being people in their homes without security expertise, and these IoT devices being always online, ever-ready to serve the botmaster, makes this is a very suitable breeding ground for launching more massive DDoS attacks.

Shifting DDoS Attack Varieties and Trends

As most typical volumetric attacks today rely on ICMP, SYN and a variety of UDP reflection and amplification attacks, the author of Mirai has interestingly introduced less common "DNS Water Torture" and "GRE flood" attacks. Though this DNS technique was already observed in the past, it's not common to see nowadays.





NCTA — The Internet & Television Association

https://www.ncta.com/sites/default/files/platform-images/wp-content/uploads/2014/05/growth-of-internet-of-things-hero-1024x585.jpg

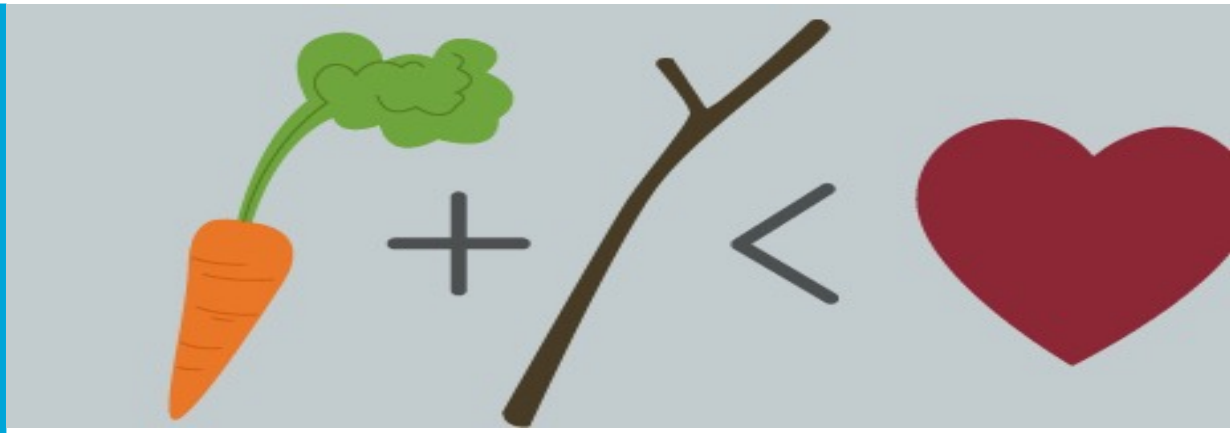
Whole Lotta Questions Raised!!

- **How?**
  - How did we get into this mess?
  - How do we get out of this mess?

How did we get here?

- Fragmented landscape
- Vendors without competence or incentives
- Lack of visibility into which ‘things’ fail
- Dependencies in value chains

How do we get out of it?
(Mopping While the Tap is Still Running)



Governance Strategies Being Discussed

- **Awareness raising**
  (but don't blame the victim)
- **Monitoring and transparency**
  (name, shame, and praise)
- **Certifications and standards**
  (FTC fining ASUS, D-Link)
- **Liability, duty to care**
  (make vendors bear the cost)
- **Intermediary Role**
  (ask ISPs to cut off access)
- **Strengthening user rights**
  (opt in, data minimization)

Governance Strategies

- Awareness raising
  (but don't blame the victim)
- Monitoring and transparency
  (name, shame, and praise)
- Certifications and standards
  (FTC fining ASUS, D-Link)
- Liability, duty to care
  (make vendors bear the cost)
- Intermediary Role
  (ask ISPs to cut off access)
- Strengthening user rights
  (opt in, data minimization)

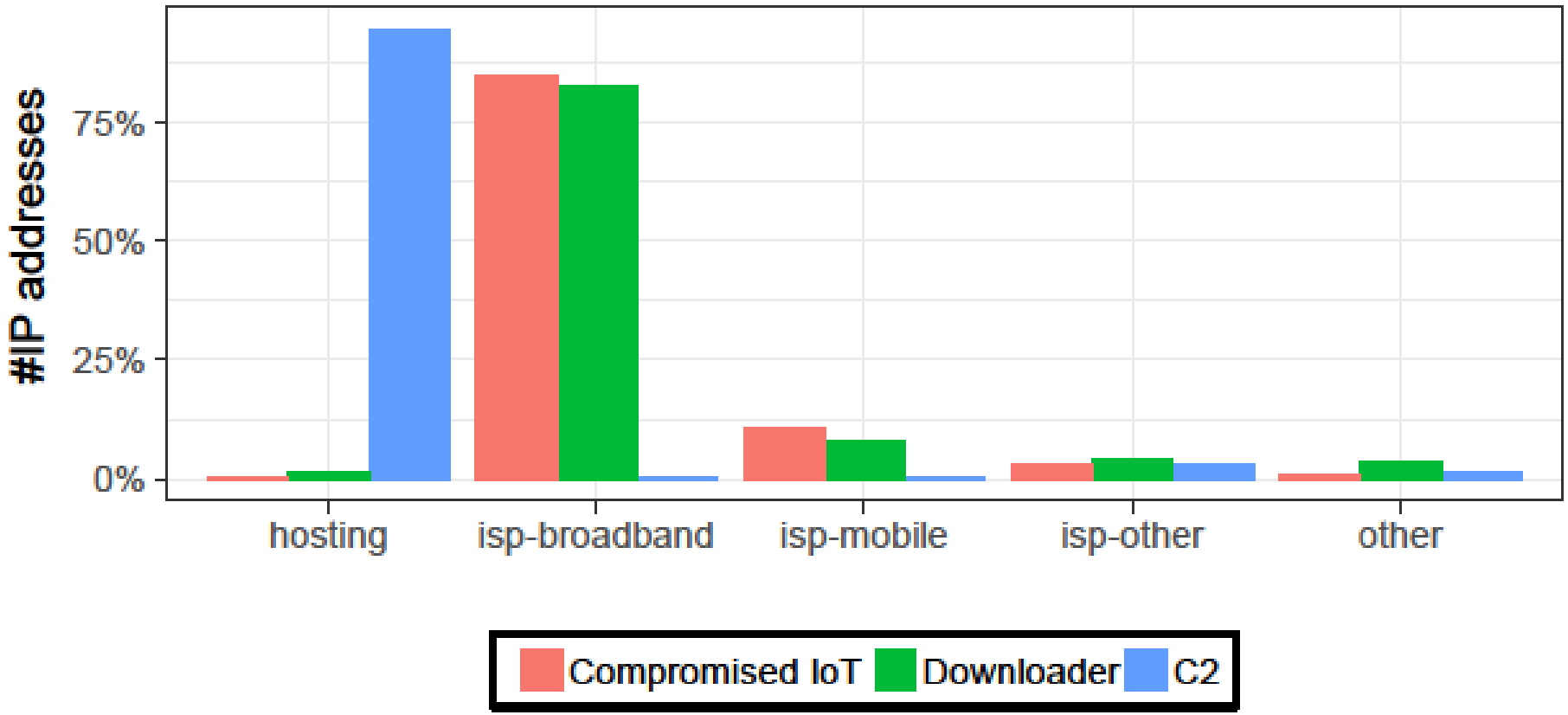
Where are the hacked devices?

TU Delft

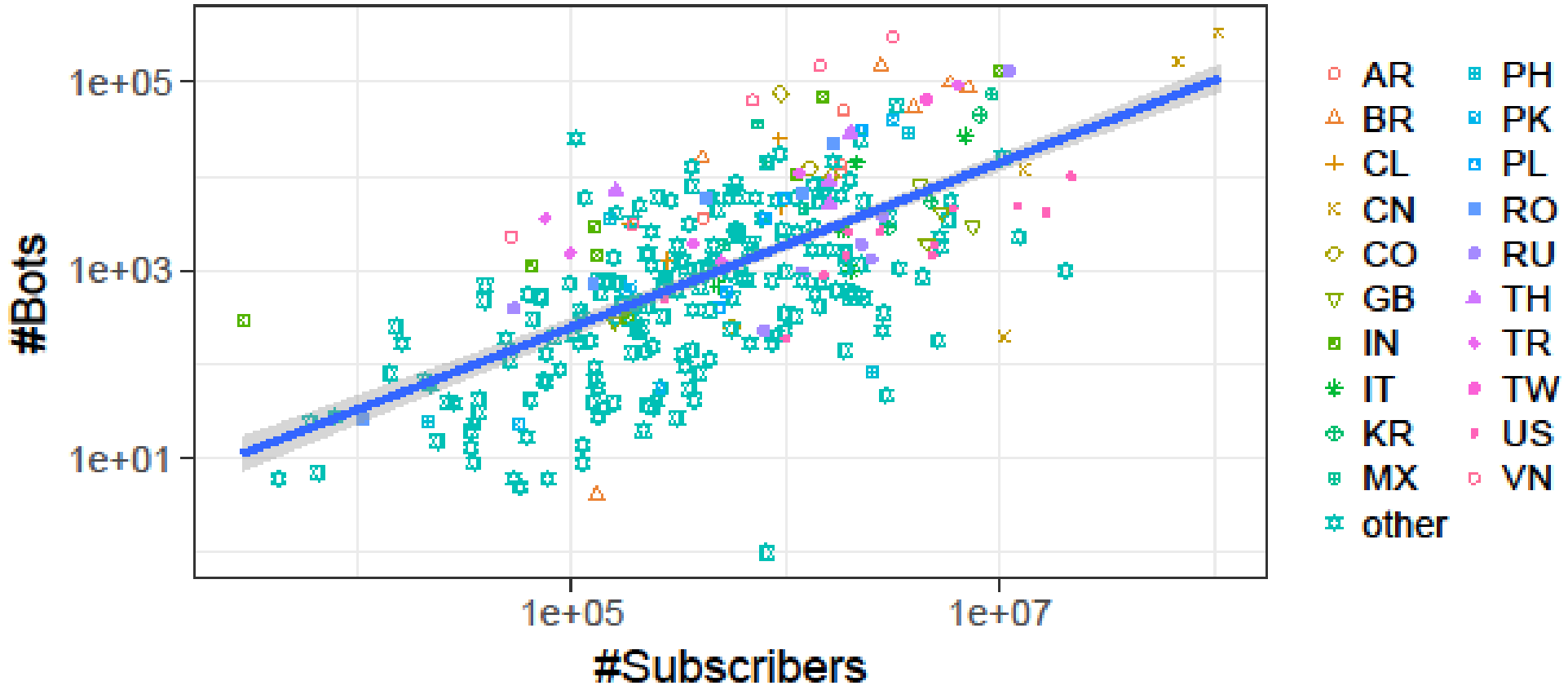
Monitoring IoT compromise

- Honeypot infrastructure with Yokohama National University (Japan)
- Emulated and physical devices
- Port 22, 23, 80, 8080, 53413, …
- Log interactions, scan back, attacking devices

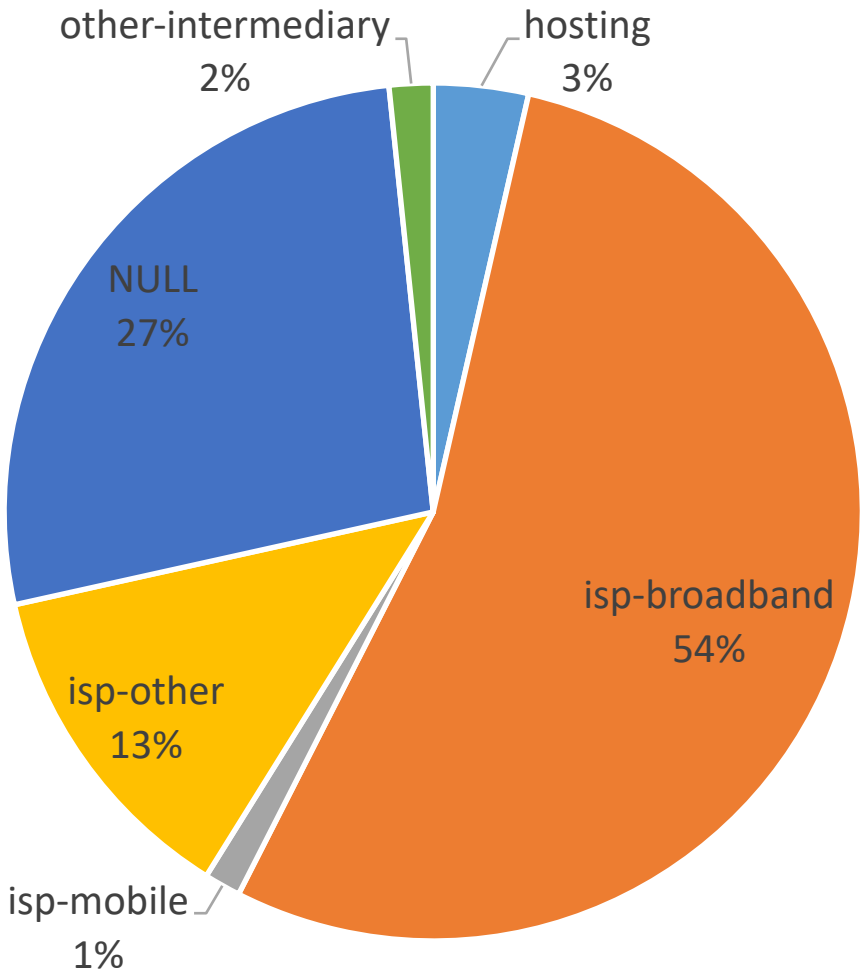
Who operates the network?



Infection rates across ISPs



Who operates the network (NL)?



Cleaning IoT Devices (KPN)

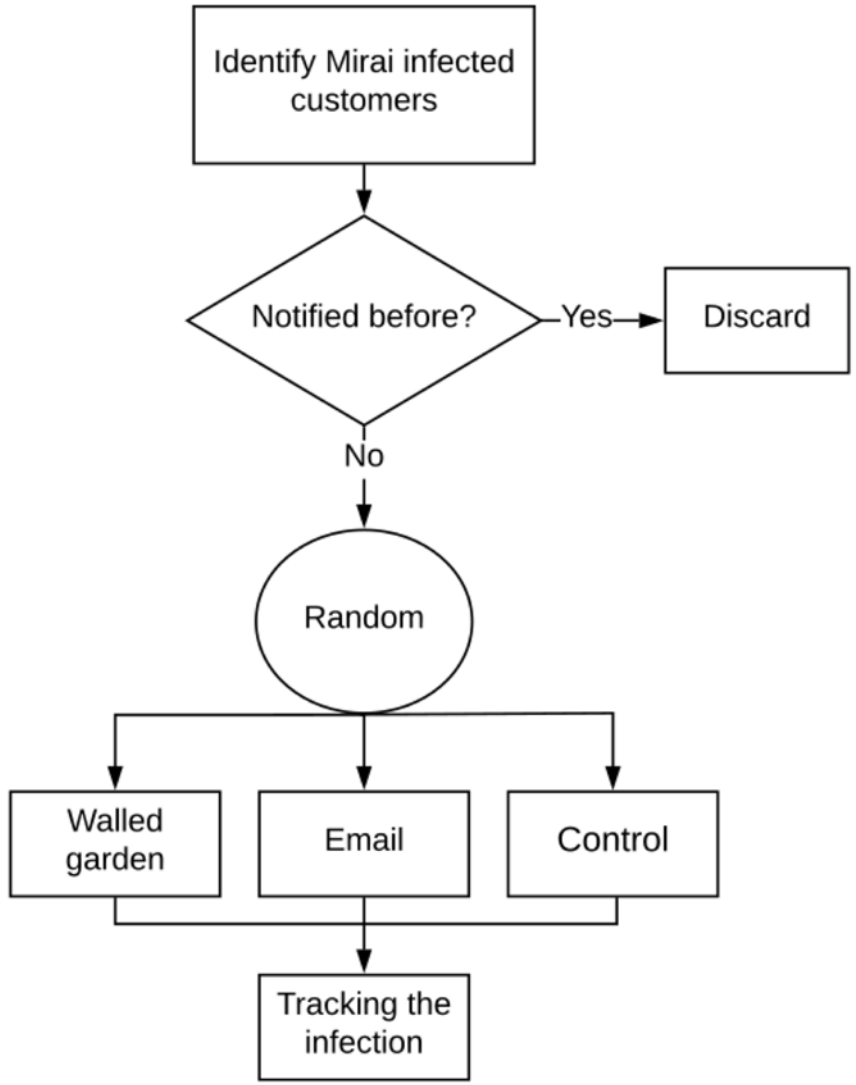
- Walled Garden
  - Cutting off access to infected devices
  - 1736 quarantining actions
  - 1208 customers
  - 50% clean infections
  - Most quarantined once

Topics	# of users
Request additional help	323 (27 %)
Request paid technician	80 (7 %)
Distrust of the notification	19 (2 %)
Complain over disruption of service	126 (10 %)
Threaten to terminate the contract	39 (3 %)
Miscellaneous	621 (51 %)

Let Me Out! Evaluating the Effectiveness of Quarantining Compromised Users in Walled Gardens.
Orçun Çetin, Lisette Altena, Carlos Gañán, Michel van Eeten. In SOUPS 2018

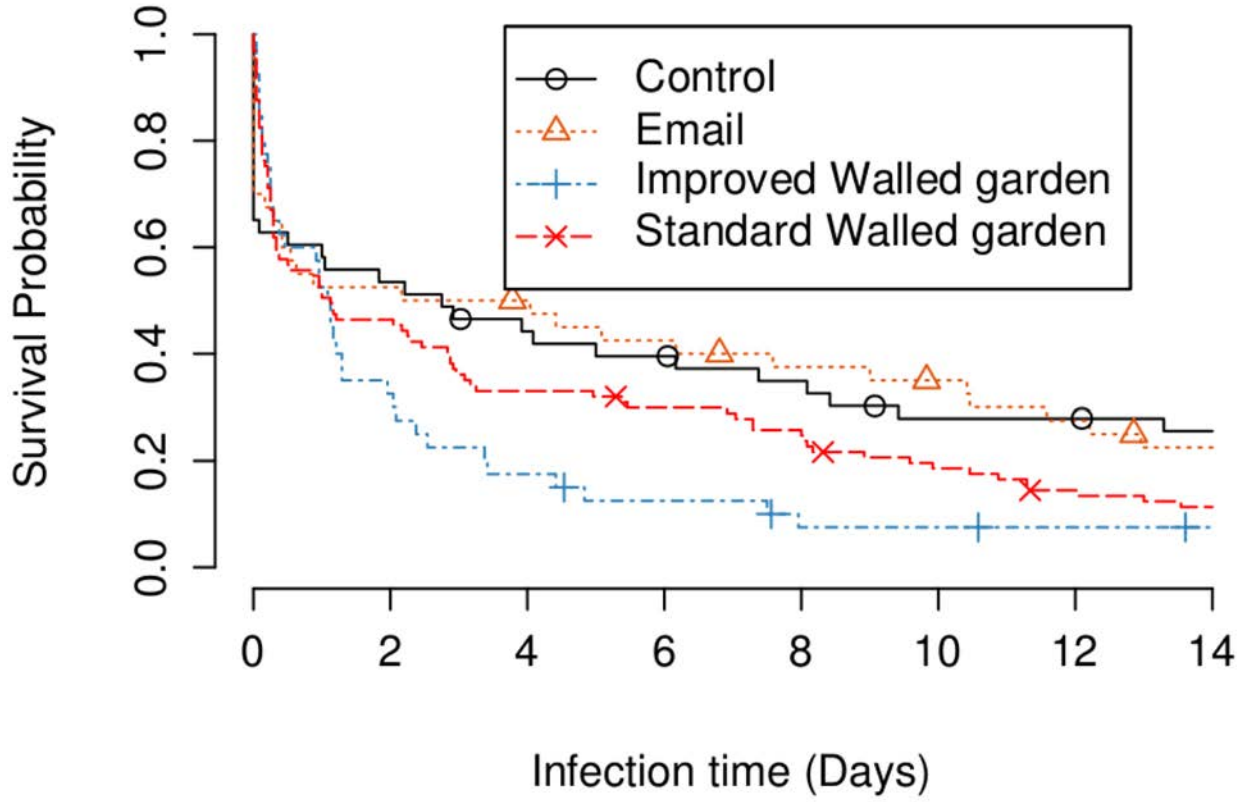
Cleaning IoT Devices (Cont.)

- Randomized Control Experiment
- 220 Customers



Cleaning IoT Devices (Cont.)

- Randomized Control Experiment
- 92% Cleaned
- In 14 days!



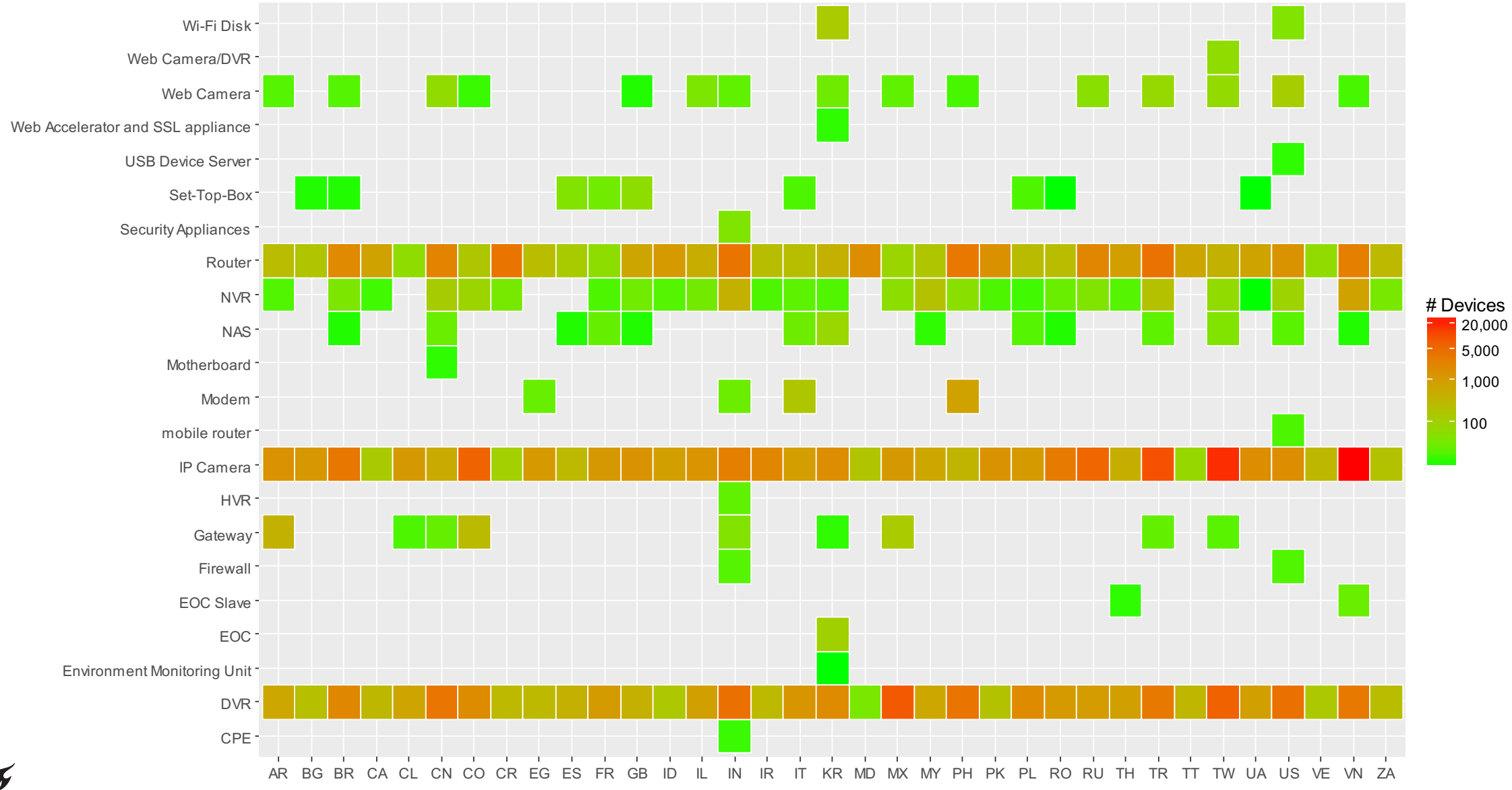
In Conclusion

Network operators can significantly help

- **Awareness raising**
  (but don't blame the victim)
- **Monitoring and transparency**
  (name, shame, and praise)
- **Certifications and standards**
  (FTC fining ASUS, D-Link)
- **Liability, duty to care**
  (make vendors bear the cost)
- **Intermediary Role**
  (ask ISPs to cut off access)
- **Strengthening user rights**
  (opt in, data minimization)

Future Research

MINIONS - MitigatINg IOt-based DDoS attacks via the DNS


Wi-Fi Disk
Web Camera/DVR
Web Camera
Web Accelerator and SSL appliance
USB Device Server
Set-Top-Box
Security Appliances
Router
NVR
NAS
Motherboard
Modem
mobile router
IP Camera
HVR
Gateway
Firewall
EOC Slave
EOC
Environment Monitoring Unit
DVR
CPE
AR BG BR CA CL CN CO CR EG ES FR GB ID IL IN IR IT KR MD MX MY PH PK PL RO RU TH TR TT TW UA US VE VN ZA
Devices
20,000
5,000
1,000
100

Thank you!

Follow our research on
https://www.tudelft.nl/cybersecurity

TU Delft