Jouw wereld. Ons domein.

Internet of Things: kansen, keerzijdes én oplossingsrichtingen

IoT webinar

3 september 2020

Doel

IoT kansrijk

Security?

Beheerder van het .nl top-level domein (TLD)

- Stichting Internet Domeinregistratie Nederland (SIDN)

- Kritische infrastructuur (‘aanbieder van essentiële diensten’)
  - Opzoeken van IP-adres van een domeinnaam (bijna elke interactie)
  - Registratie van alle .nl-domeinnamen
  - Beheren van een fouttolerante en gedistribueerde infrastructuur

- Waarde van het Internet voor Nederland en daarbuiten vergroten
  - Veilig en nieuw gebruik van het Internet mogelijk maken
  - Veiligheid en weerbaarheid van het Internet zelf verbeteren

.nl = the Netherlands
17M inhabitants
6M domain names
3.3M DNSSEC-signed
2B+ DNS queries/day
stats.sidnlabs.nl

SIDN fonds

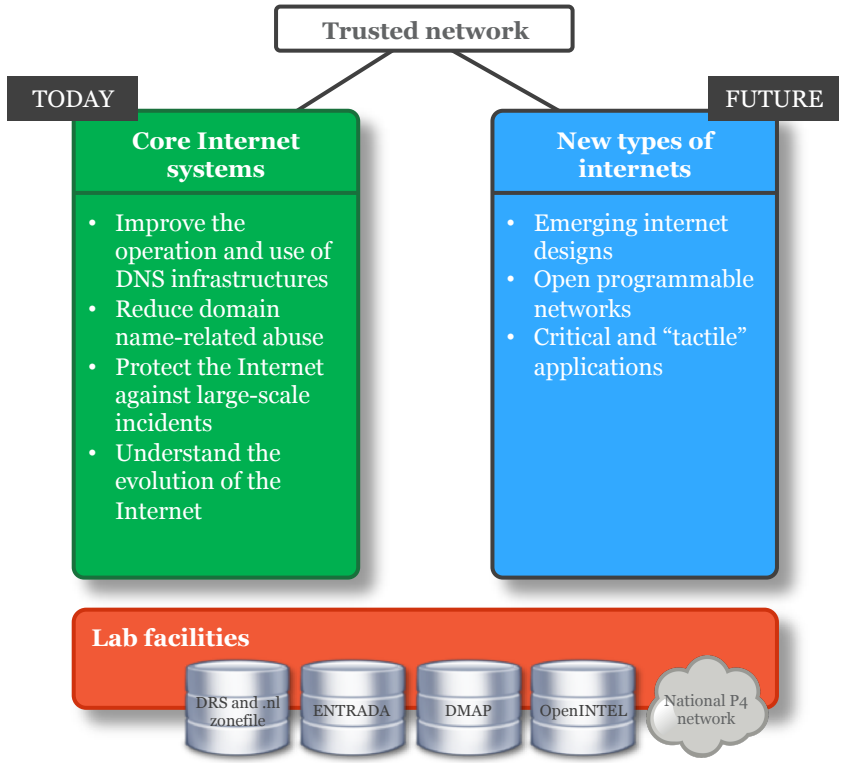
SIDN LABS

Doel SIDN Labs: verhogen van de betrouwbaarheid van de internetinfrastructuur van onze samenleving

- Betrouwbaar = veilig, stabiel, weerbaar en transparant, voor .nl en NL in het bijzonder

- Strategieën om dat te bereiken
  - Toegepast onderzoek (meten, prototypen, evalueren) o.b.v. gevalideerde onderzoeksagenda
  - Versterken onderzoek- en operationele communities (SIDN, NL, EU, wereldwijd), bijv. door delen resultaten

- 2020's: grip op publieke waarden van NL en EU zoals privacy en safety ('digitale soevereiniteit')



Dagelijks werk

- Operationele teams helpen
- Open source software schrijven
- Grote hoeveelheden data analyseren
- Experimenten draaien
- Academische artikelen en technische rapporten schrijven
- Samenwerken met universiteiten

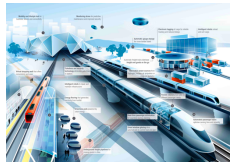
SIDN LABS

Voorbeelden van onderzoekpartners

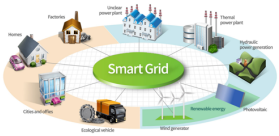
Internet of Things (IoT)

- Internet application that extends “network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered to be computers” [ISOC]

- Differences with “traditional” applications
  - IoT continually senses, interprets, acts upon physical world
  - Without user awareness or involvement (passive interaction)
  - 20-30B devices “in the background” of people’s daily lives
  - Widely heterogeneous (hardware, OS, network connections)
  - Longer lifetimes (perhaps decades) and unattended operation



Intelligent Transport Systems



Smart energy grids

Smart homes and cities

- IoT promises a safer, smarter, and more sustainable society

[ISOC] K. Rose, S. Eldridge, L. Chapin, “The Internet of Things: An Overview – Understanding the Issues and Challenges of a More Connected World”, ISOC Whitepaper

Kansen

IoT CHANGES EVERYTHING

SDN LABS

Smart Solutions

E-Governance and Citizen Services

1. Public Information, Grievance Redressal
2. Electronic Service Delivery
3. Citizen Engagement
4. Citizens - City's Eyes and Ears
5. Video Crime Monitoring

Waste Management

6. Waste to Energy & fuel
7. Waste to Compost
8. Waste Water to be Treated
9. Recycling and Reduction of C&D Waste

Water Management

10. Smart Meters & Management
11. Leakage Identification, Preventive Maint.
12. Water Quality Monitoring

Energy Management

13. Smart Meters & Management
14. Renewable Sources of Energy
15. Energy Efficient & Green Buildings

Urban Mobility

16. Smart Parking
17. Intelligent Traffic Management
18. Integrated Multi-Modal Transport

Others

19. Tele-Medicine & Tele Education
20. Incubation/Trade Facilitation Centers
21. Skill Development Centers

SDN LABS

Voorbeeld: home automation

Automatisering

Backend in cloud

Keerzijdes


YOU GET CONNECTED!
AND YOU GET CONNECTED!
EVERYTHING GETS CONNECTED!
imgflip.com

Keerzijdes

Home > Data Protection > Internet of Things

SLIDESHOW

The internet of insecure things: Thousands of internet-connected devices are a security disaster in the making

By Josh Fruhlinger, CSO | Oct 12, 2016 4:00 AM PT

Keerzijdes

NEWS

More than two-thirds of consumers are concerned about IoT device security

By Sooraj Shah - April 27, 2017

Source: Internet of business

Stelling

Ik doe actief onderzoek naar de beveiliging bij aanschaf van een IoT product.

A Eens

B Oneens

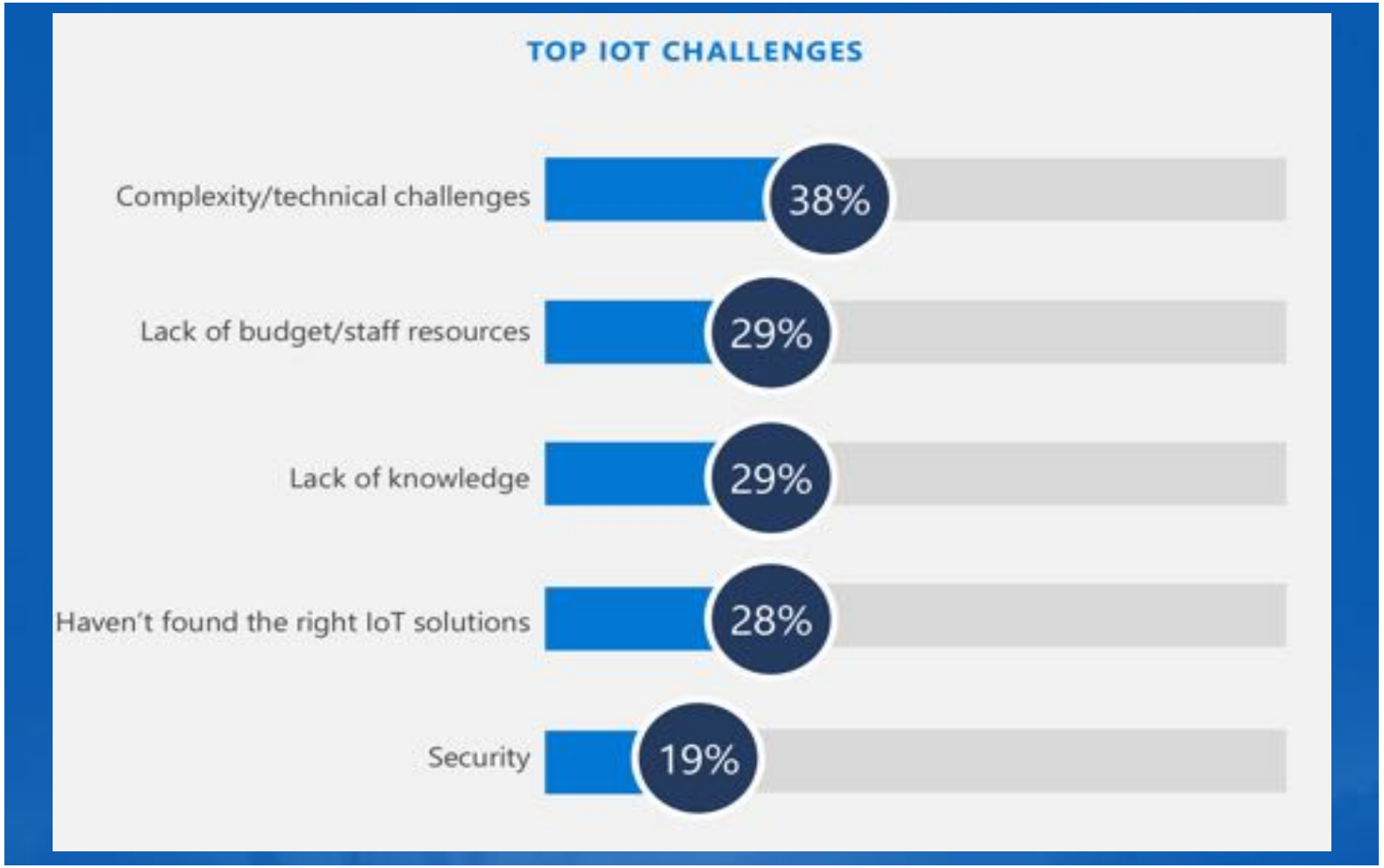
Enquête over IoT-uitrol bij bedrijven

Enquête over IoT-uitrol bij bedrijven

"Security concerns around IoT adoption are universal: 97% of companies are concerned about security when implementing IoT"

Enquête over IoT-uitrol bij bedrijven

"Security concerns around IoT adoption are universal: 97% of companies are concerned about security when implementing IoT (though this is not hindering adoption)"



Privacy

rtlnieuws

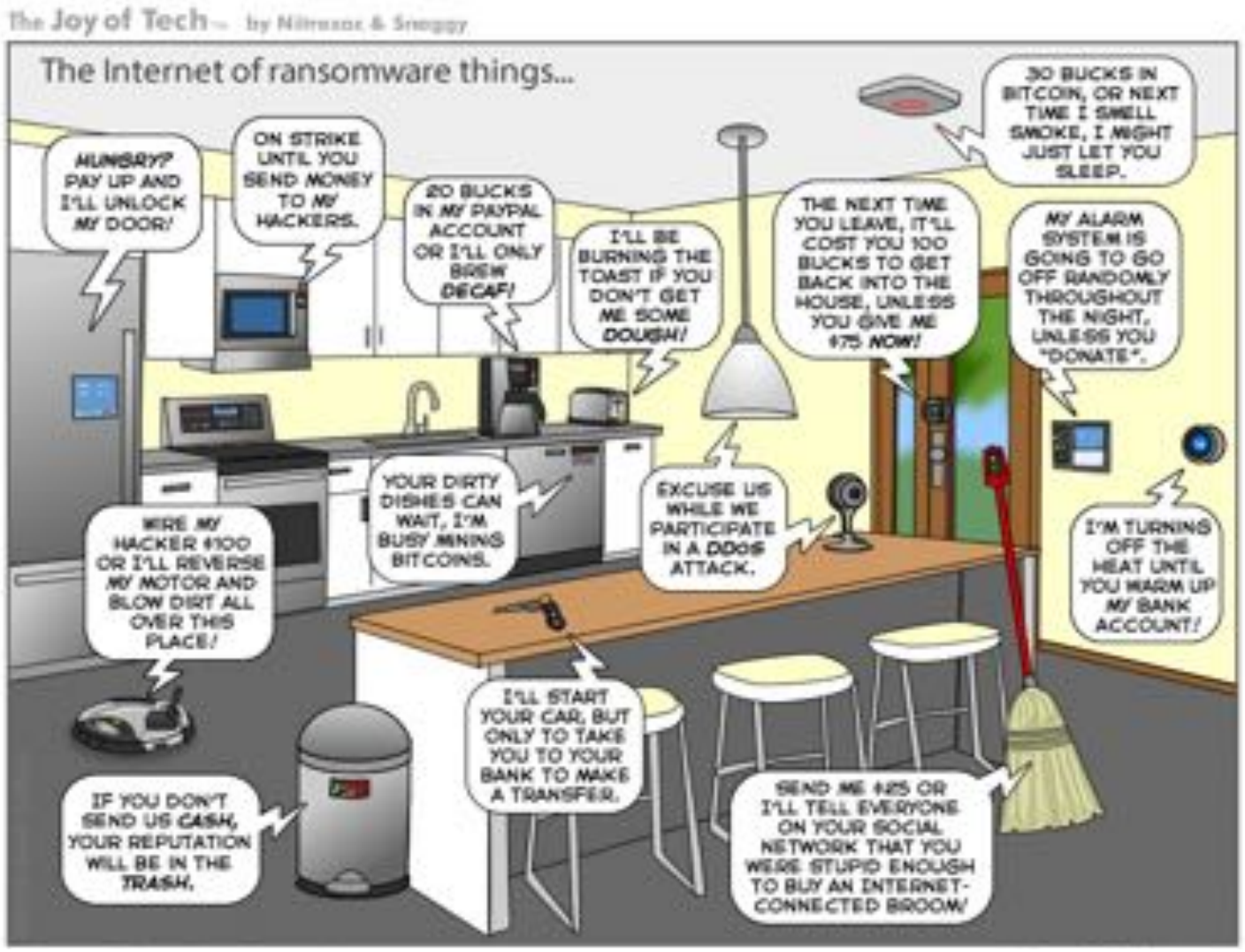
EXCLUSIEF

Gluren in babykamers: duizenden slimme camera's in Nederland onveilig door lek

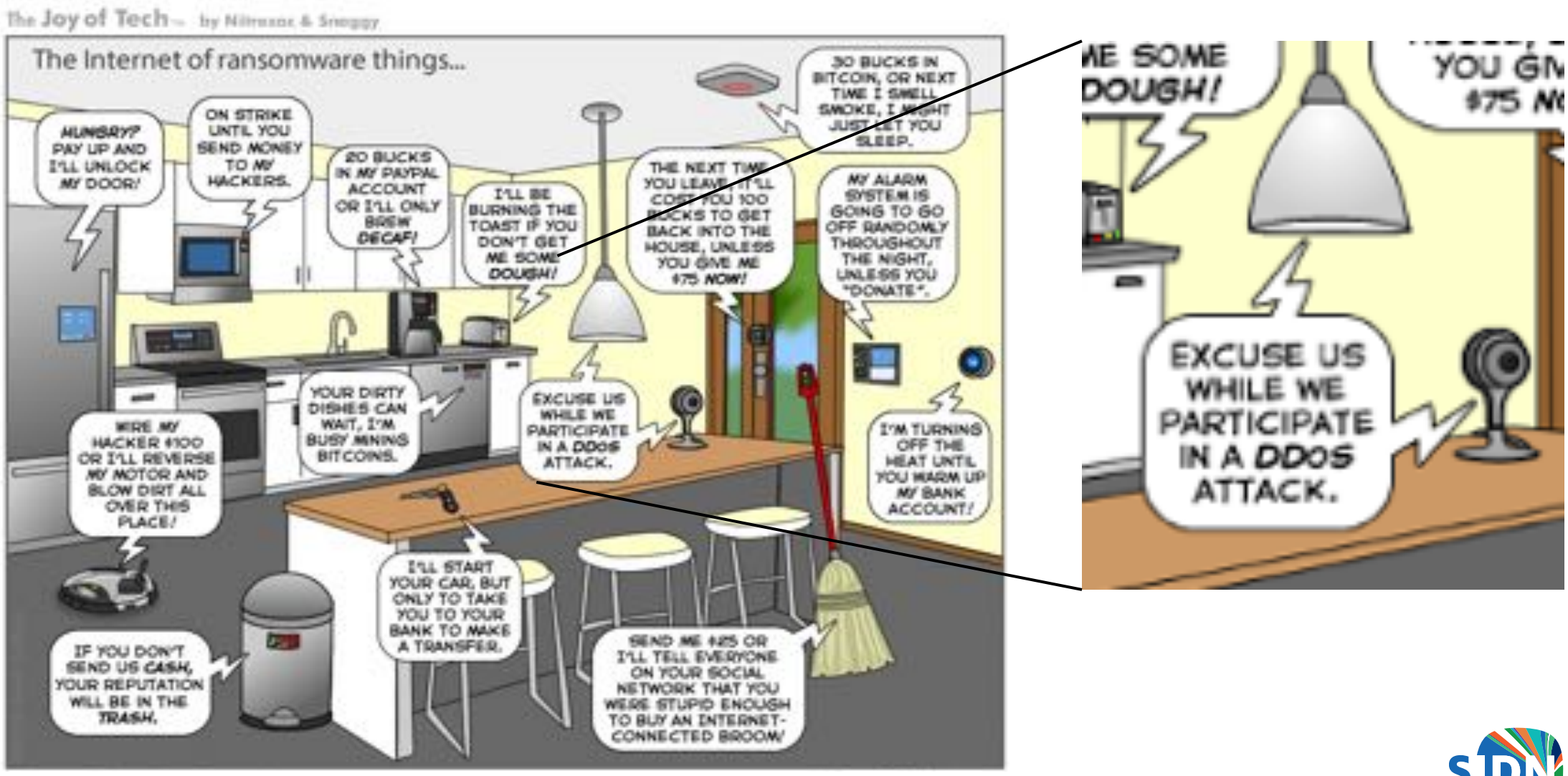
Aangepast: 21 september 2019 12:05

Kwaadwillenden kunnen meegluren met duizenden Nederlandse beveiligingscamera's en babyfoons. Door een lek liggen e-

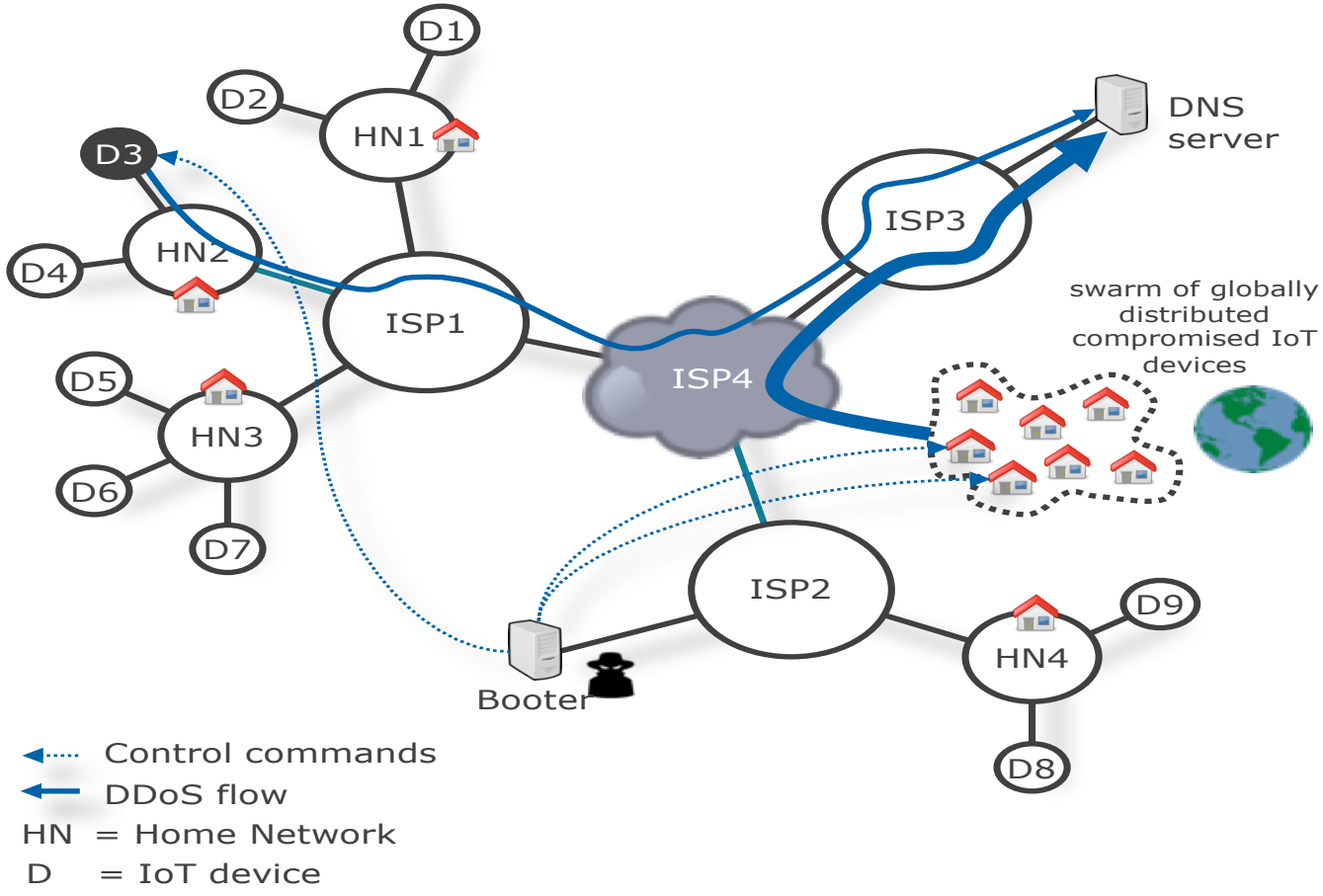
“The Connected Home of the Future”



“The Connected Home of the Future”



IoT 'wakeup call' voor ccTLDs en andere beheerders: Mirai-powered DDoS aanvallen

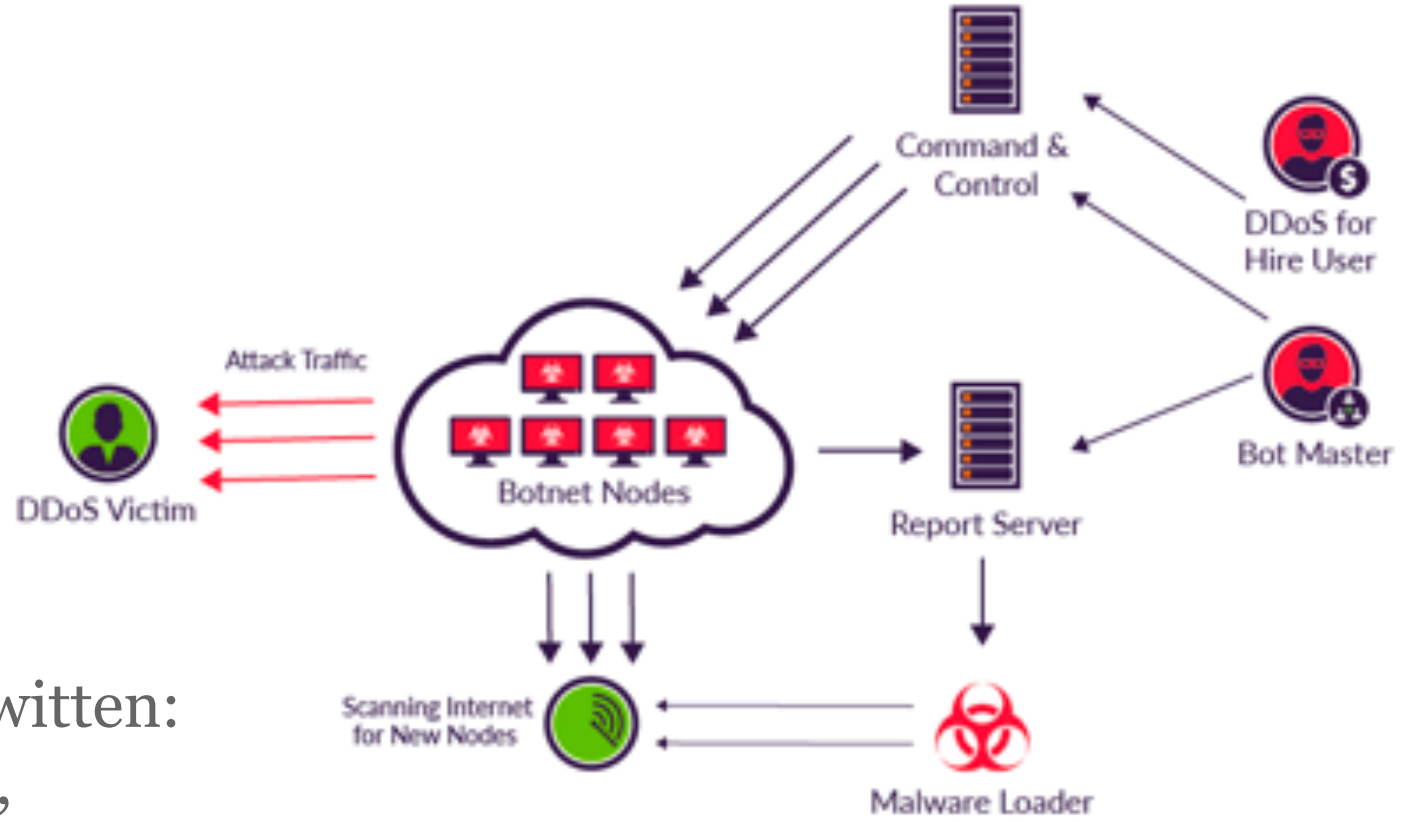


Other targets: OVH (hosting provider), Krebs On Security (website), Deutsche Telecom (ISP)

Sources:
[Mirai17], [Hajime19], [SAC105]
https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
https://www.zdnet.com/article/mirai-botnet-attack-briefly-knocked-an-entire-country-offline/

Mirai DDoS aanvallen

- Meeste doelwitten in VS (50%), Frankrijk, VK.
- Games
- Mirai C2 servers



- High-profile doelwitten:
  Krebs on Security,
  Lonestar Cell (Liberia), Dyn.

Quiz

Botnets worden niet alleen voor DDoS-aanvallen gebruikt

Voor welke andere activiteit werd het Mirai botnet ook gebruikt?

A Bitcoin mining

B Versturen van spam

C Delen van films

D Klikfraude

Quiz

Botnets worden niet alleen voor DDoS-aanvallen gebruikt

Voor welke andere activiteit werd het Mirai botnet ook gebruikt?

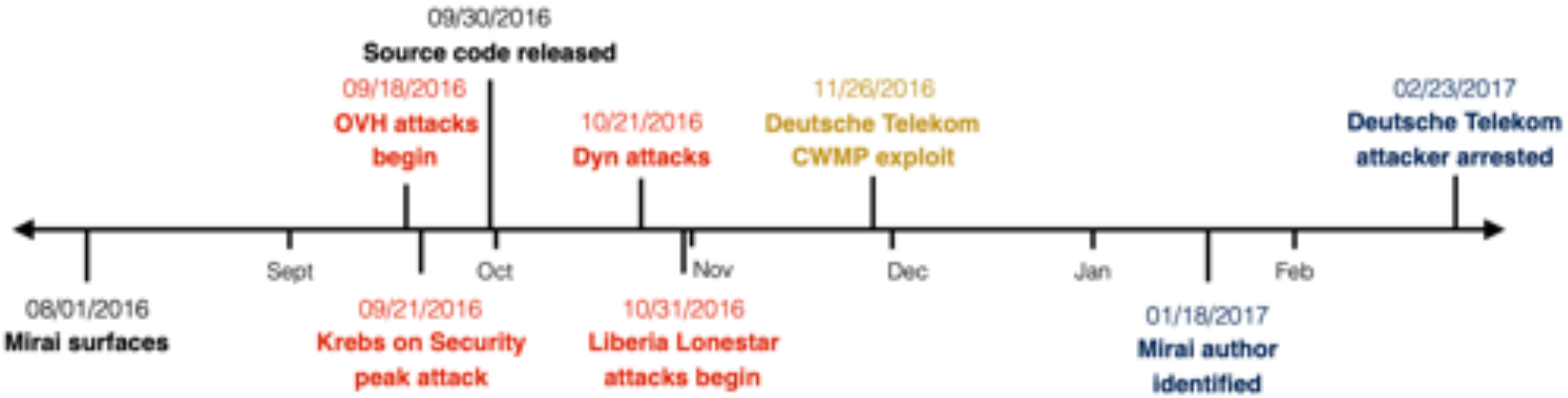
A Bitcoin mining

B Versturen van spam

C Delen van films

D Klikfraude

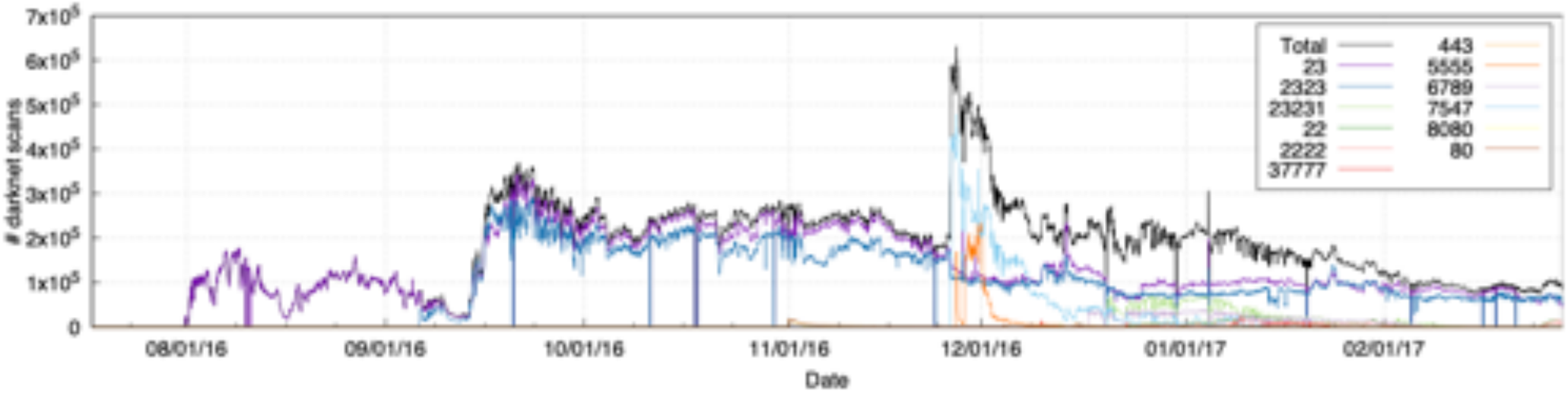
De beginjaren van Mirai



M. Antonakakis et al., “Understanding the Mirai Botnet”, in: 26th USENIX Security Symposium, 2017

Mirai vanuit het network gezien

- Actief scannen: Censys
- IoT Honeypot: 1028 unieke samples en 67 C2 domeinen
- Passieve en Actieve DNS gebruiken om C2 servers te vinden
- C2 milker: 15.000 aanvallen



M. Antonakakis et al., “Understanding the Mirai Botnet”, in: 26th USENIX Security Symposium, 2017

Quiz

Hoeveel hosts met Mirai (+varianten) zijn in 2019 nog steeds actief (SYN scan)?

A 0

B 5k

C 20k

D 50k

Quiz

Hoeveel hosts met Mirai (+varianten) zijn in 2019 nog steeds actief (SYN scan)?

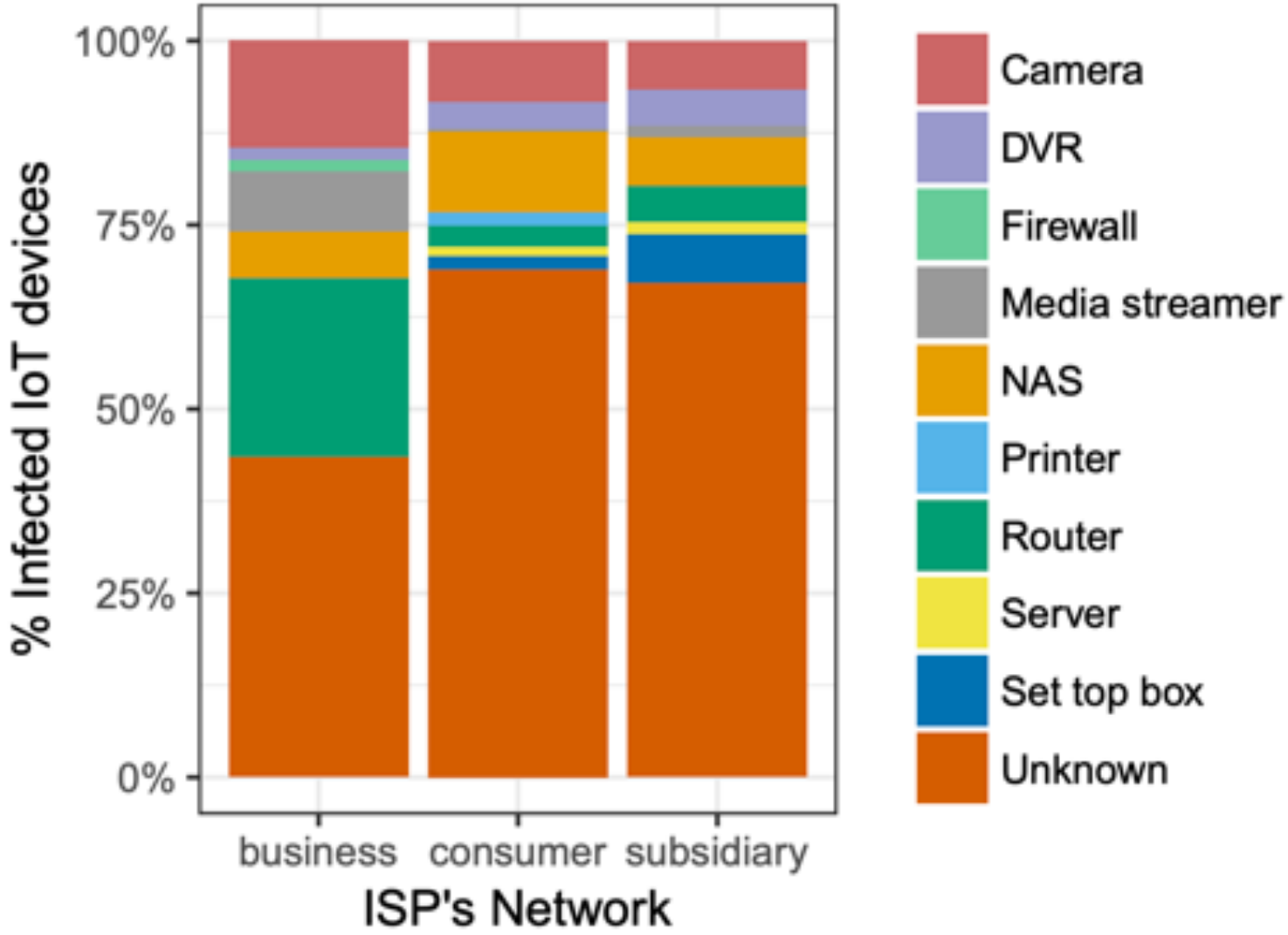
A 0

B 5k

C 20k

D 50k

Geïnfecteerde apparaten



O. Cetin et al., “Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai”, in: NDSS 2019

Hajime: infecties door de tijd

March 24, 2018
Chimay-Red exploit
From 43K to 71K/93K

May 8, 2018
GPON exploit
To 96K
"?images" append

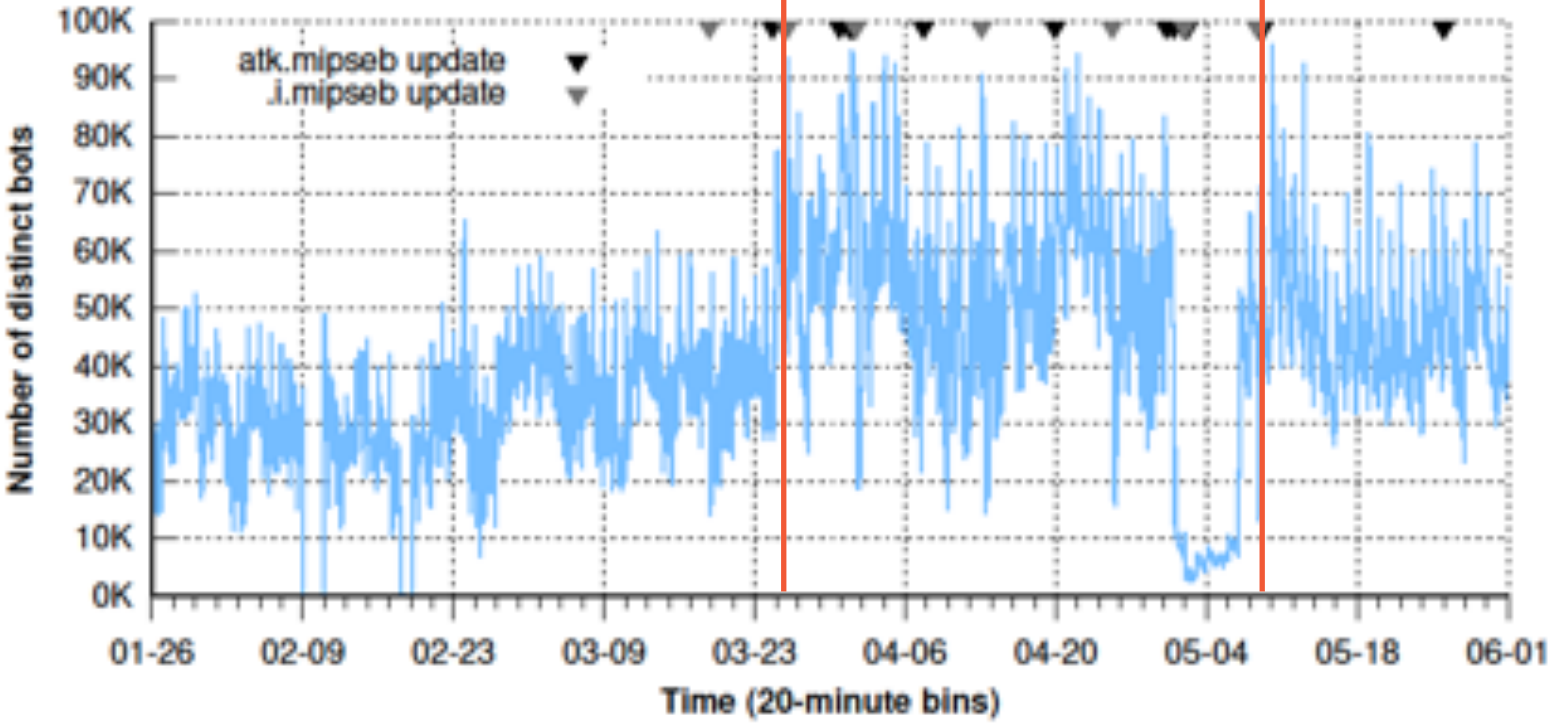


Fig. 2: Number of unique Hajime bots. (Active scans.)

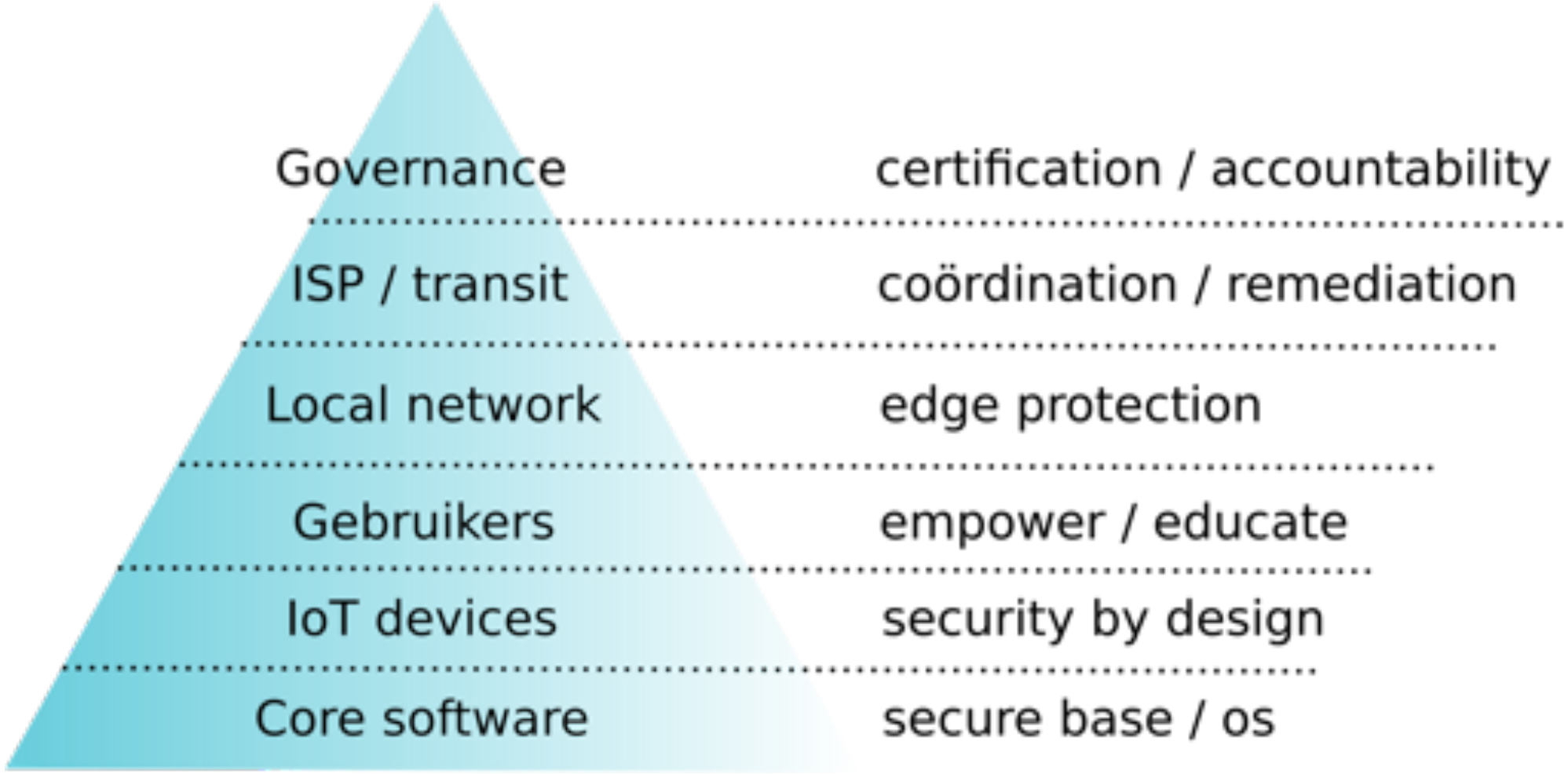
S. Herwig et al., "Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet", Network and Distributed Systems Security (NDSS) Symposium 2019

Andere IoT botnets

Botnet	Geschatte piek
Mirai	600k
Hajime	96k
Anarchy	11k
Reaper	10k-20k
Kepler / JenX / Torii	?
BrickerBot	n.v.t.

Oplossingsrichtingen

Wat moet er gebeuren?



Oplossingsrichtingen: wetgeving en certificering

Foto: IoT testbed uit J. Reng et al, “Information Exposure From Consumer IoT Devices”, in: IMC 2019

Oplossingsrichtingen: certificering?

DIGITALEUROPE

24 OCTOBER 2019

Defining the way forward for IoT security and certification schemes

Executive Summary

This document aims to provide guidance on how to address cybersecurity of the Internet of Things (IoT) in the context of the adoption of future cybersecurity schemes under the Cybersecurity Act, and other relevant European legislation. Our goal is to advance more effective cyber risk management across the European Digital Single Market.

https://www.digitaleurope.org/resources/defining-the-way-forward-for-iot-security-and-certification-schemes/

SIDN LABS

Oplossingsrichtingen: verbieden?

NOS Nieuws Sport Uitzendingen TELEBLIK AEX 28 km 5°

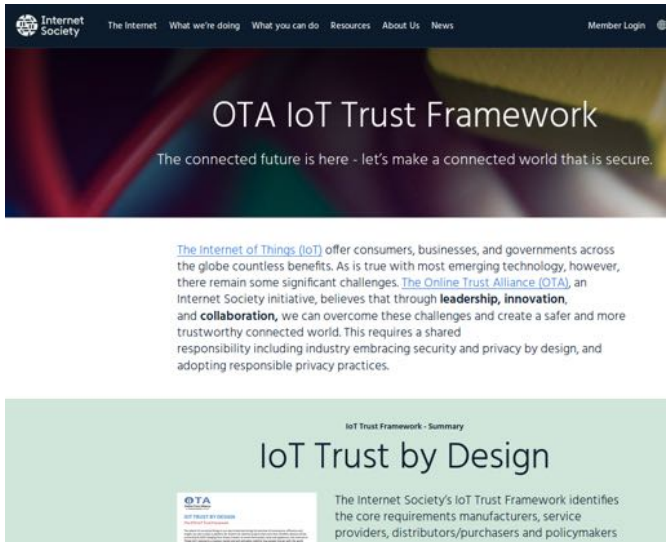
Adviesraad kabinet: verbod op onveilige 'slimme' apparaten

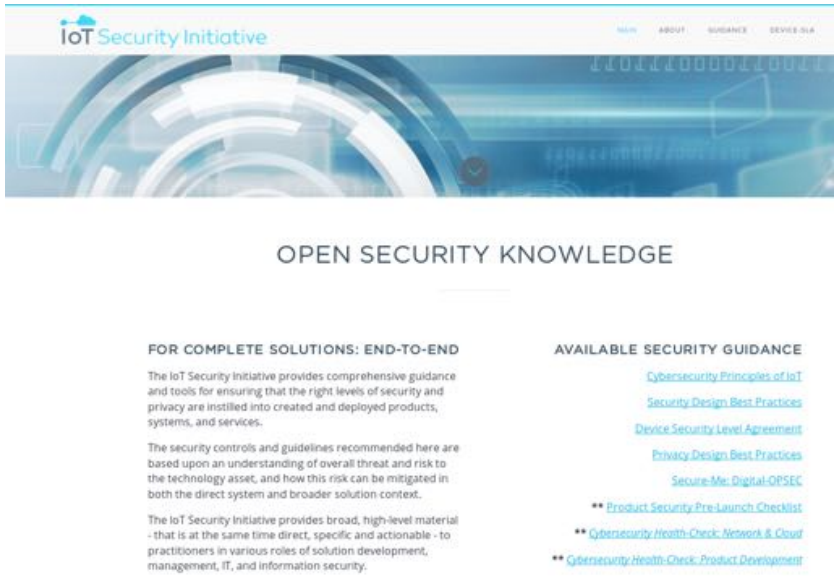
Joost Schellevis

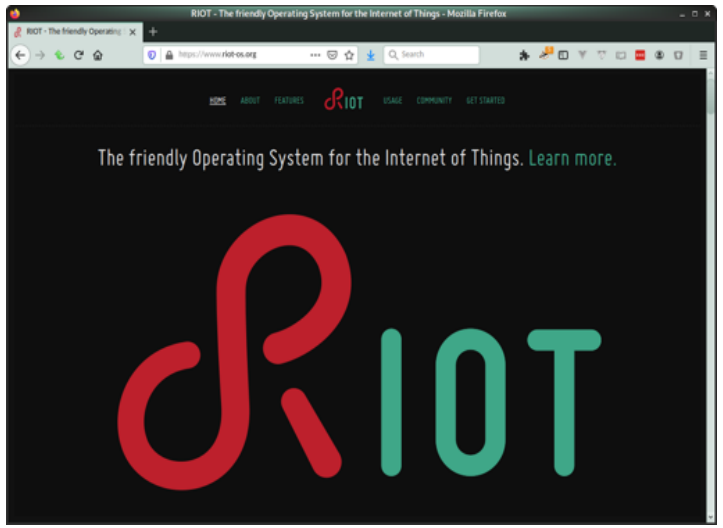
ANP

Het kabinet moet onderzoeken of onveilige *internet of things*-apparaten geweerd kunnen worden van de markt. Daarvoor pleit de Cyber Security Raad, een adviesorgaan van het kabinet. In die raad zitten mensen uit het bedrijfsleven, de wetenschap en de overheid.

(Andere) initiatieven wereldwijd, verschillende niveaus







Oplossingsrichtingen: beschermen en opschonen

Artikel: Cleaning up the Internet of Evil Things

Artikel van TUD, YNU en NICT over de effectiviteit van strategieën om botnets op te schonen, zoals de gebruiker informeren en aansluitingen in quarantaine zetten.

Het onderzoek meette via diverse databronnen het aantal mirai-besmettingen, en de hoeveel er opgeschoond werd.

O. Cetin et al., “Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai”, in: NDSS 2019

Paper: Cleaning up the Internet of Evil Things

- 87% van de besmettingen in breedbandaansluitingen
- 58-74% natuurlijk verloop (verdween zonder verdere actie van de onderzoekers) bij diverse controlegroepen
- 77% opgeschoond na e-mail berichtgeving
- 92% opgeschoond na quarantaine
- 5% opnieuw geïnfecteerd na 5 maanden

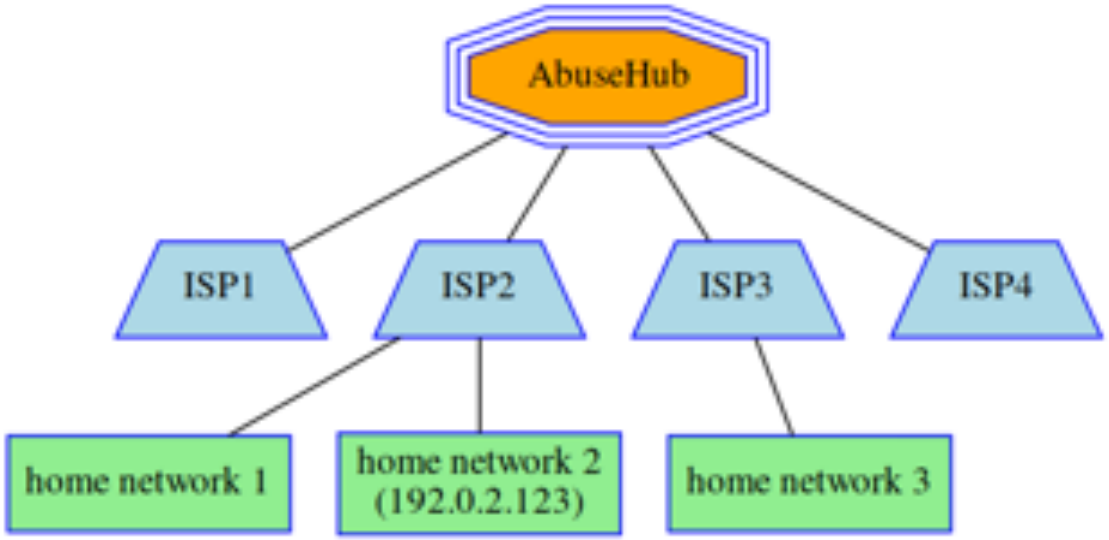
O. Cetin et al., “Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai”, in: NDSS 2019

Conclusie

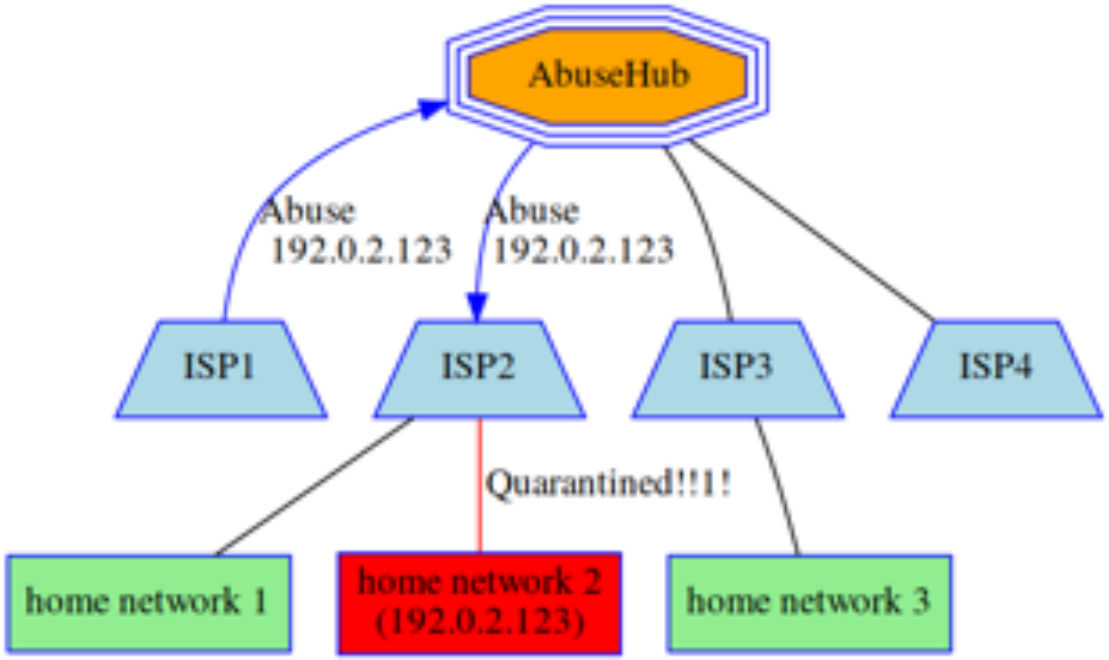
- Quarantaines werken!

- Ze moeten wel goed uitgevoerd worden
  - Vermelding oorzaak
  - Vermelding datum en tijd
  - Vermelding wat gebruiker kan doen

Quarantaine

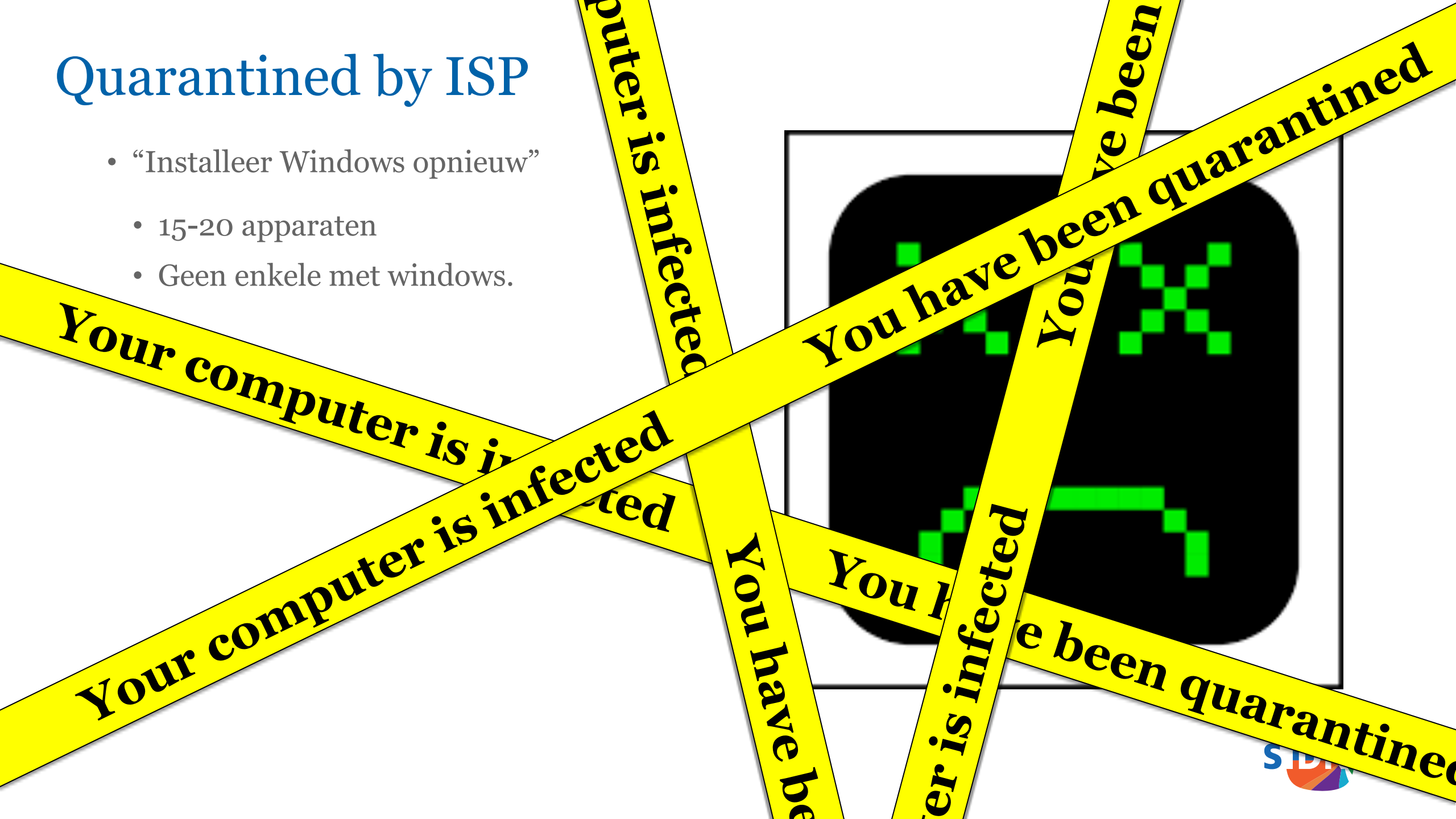


Quarantaine

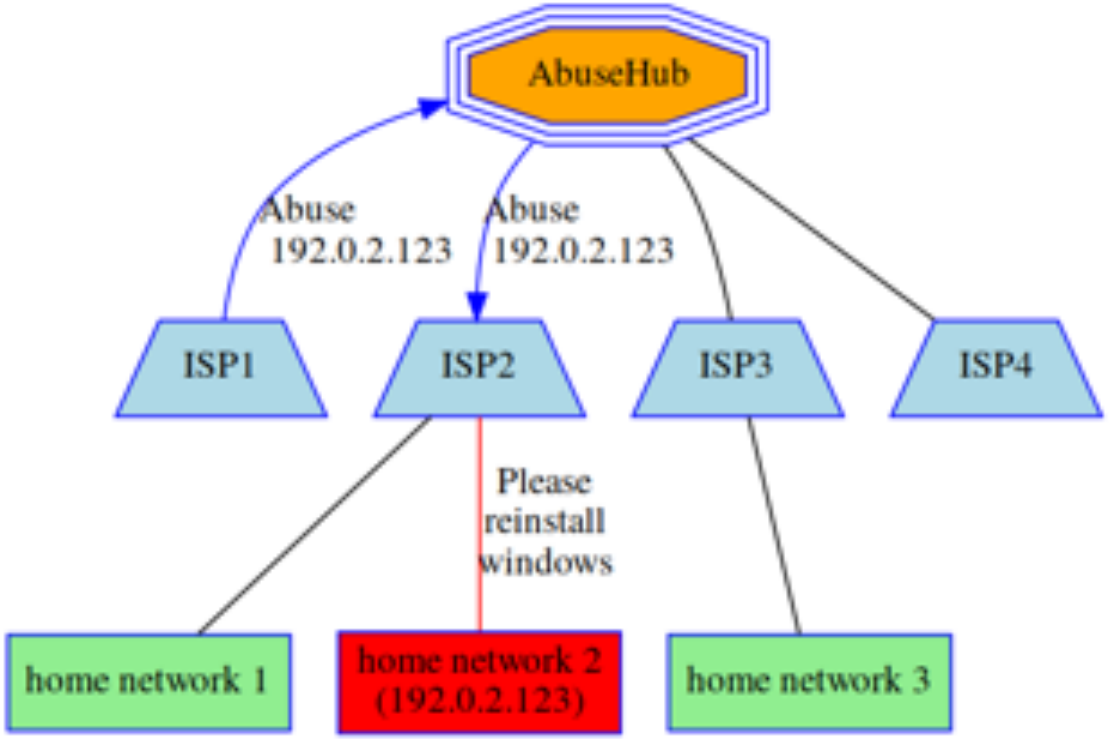


Quarantined by ISP

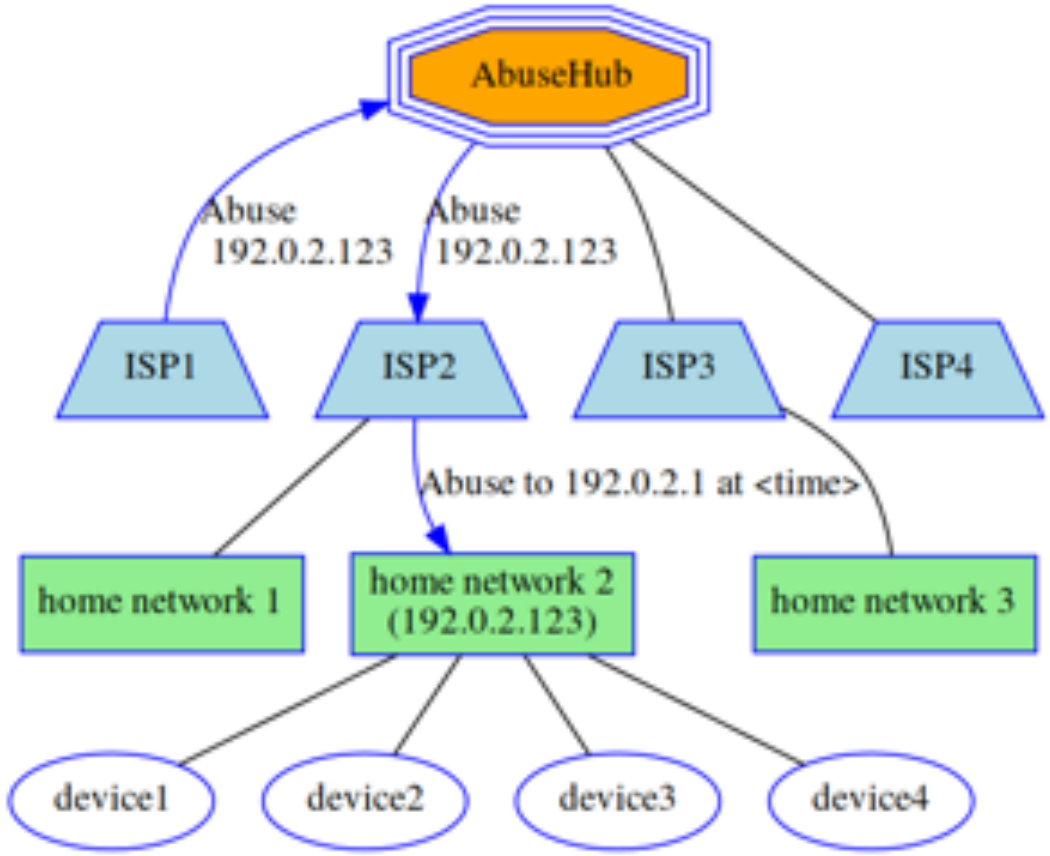
- “Installeer Windows opnieuw”
  - 15-20 apparaten
  - Geen enkele met windows.



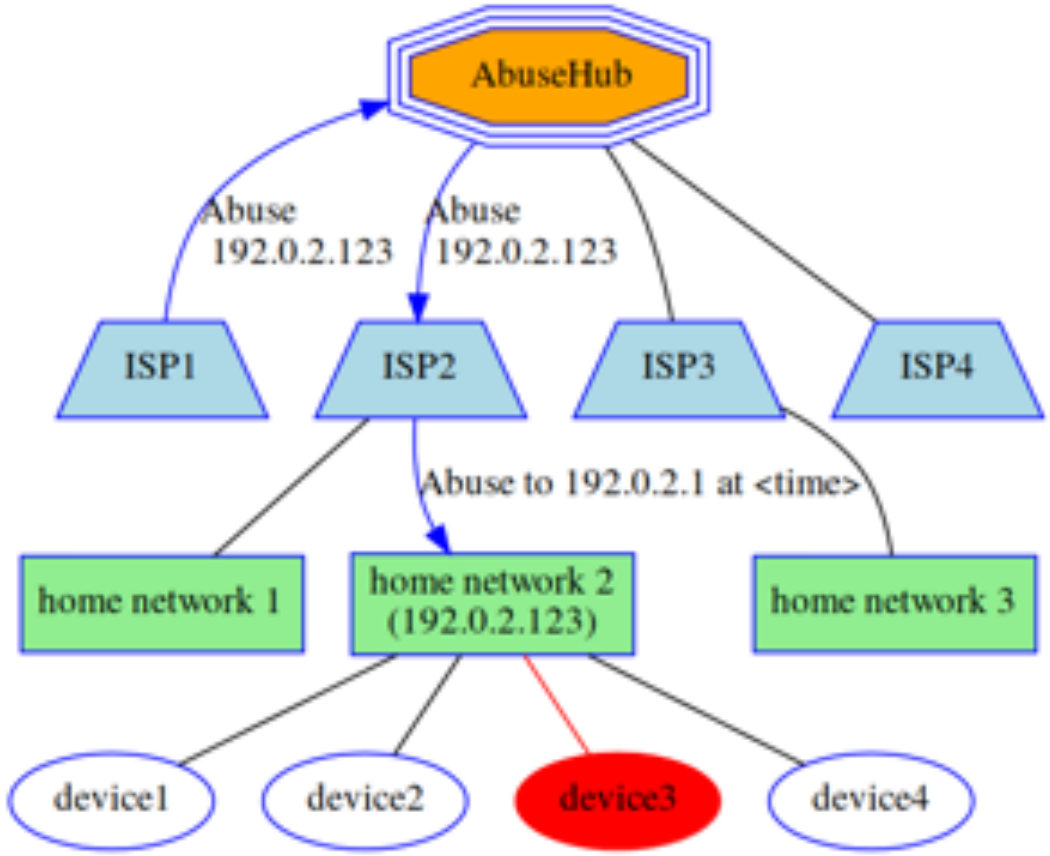
Idee: Incident report system



Idee: Incident report system



Idee: Incident report system



Granulaire quarantaine

- Systeem meldt het kwaadaardige netwerkgedrag
- Router bepaalt hoe te verhelpen
  - Preventieve firewall-regels
  - Actieve respons op meldingen (apparaatquarantaine)

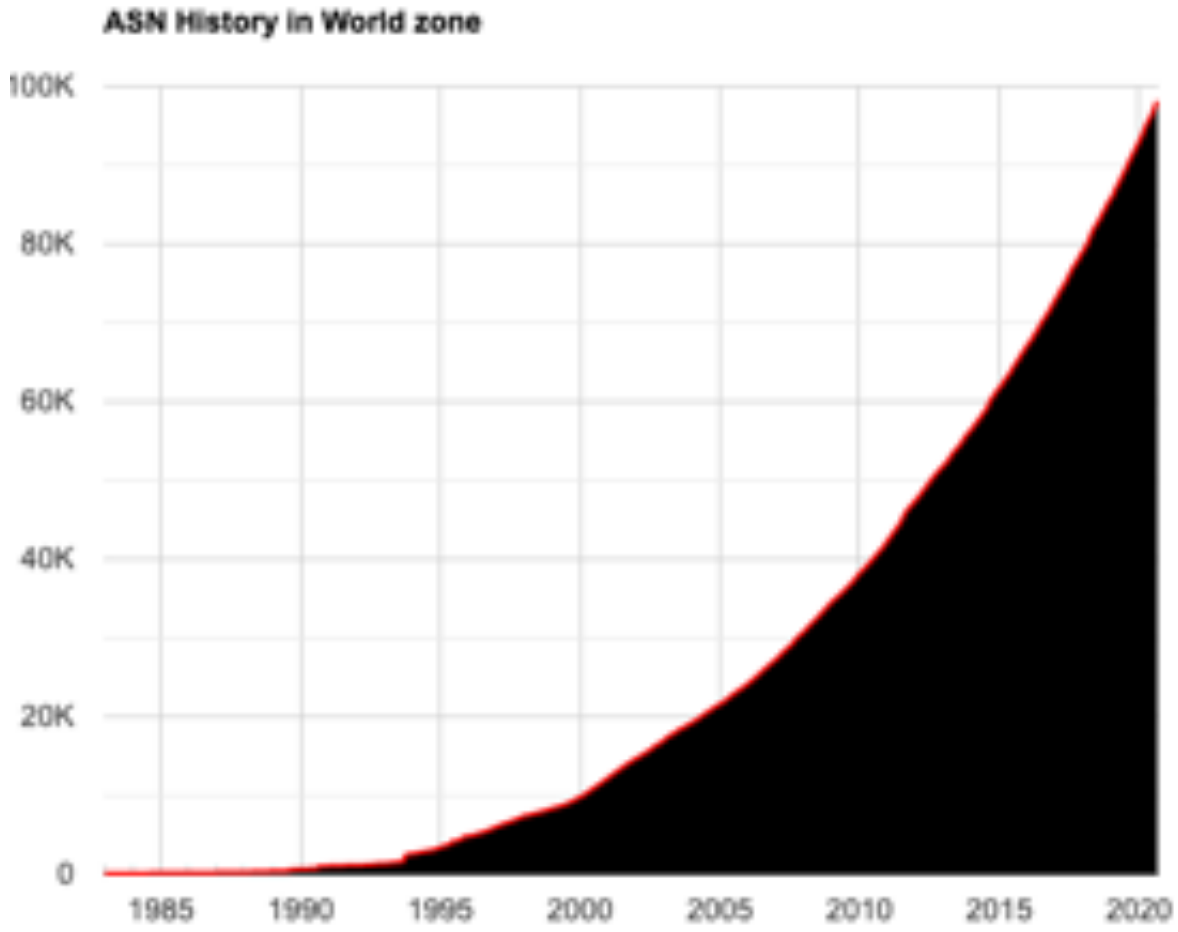
- DDoS Open Threat Signaling (DOTS) bij IETF
  - https://datatracker.ietf.org/wg/dots/charter/
  - https://datatracker.ietf.org/doc/draft-ietf-dots-signal-call-home

SIDN LABS

Samenwerken tussen ISP's van belang!

98k Autonomous Systems

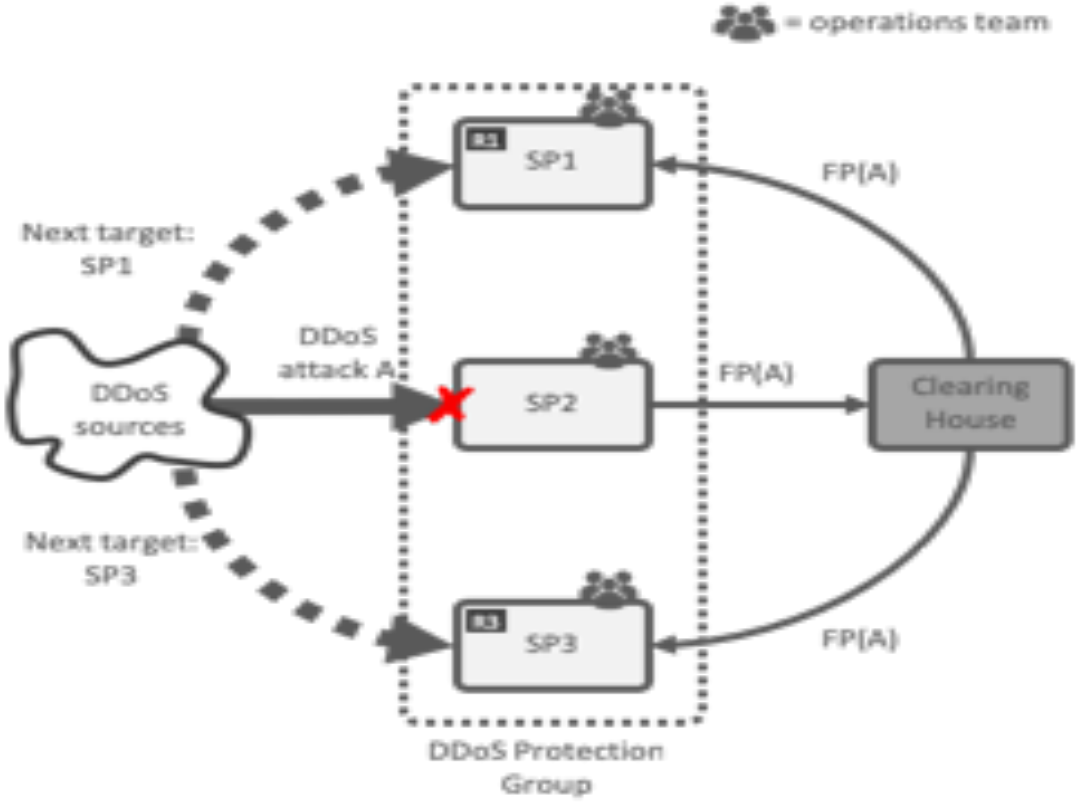
Iedereen ziet deel
(DNS, routing, abuse feeds)



Grafiek: Patrick Maigron, "World - Autonomous System Number statistics", 31 augustus 2020

Voorbeeld: DDoS clearing house

- Pilot over hoe ISP's kunnen samenwerken om DDoS actief te bestrijden
- Doorlopend en automatisch delen van "fingerprints" van DDoS-aanvallen kan providers proactief laten mitigeren
- Aanvullend op 'standaard' DDoS-bescherming zoals de NaWas of Cloudflare
- Pilot met 10 NL partners, daarna opschaling naar EU-level in het CONCORDIA project [DDoS19]



The work of SIDN, SURFnet, and the University of Twente on the DDoS clearing house was partly funded by the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927.

Oplossingsrichtingen: veiligere thuisnetwerken

Veiligheidsanalyses van apparatuur

Analyses om consumenten te helpen

https://www.agentschaptelecom.nl/documenten/rapporten/2019/09/25/rapport-digitale-veiligheid-van-iot-apparatuur

4 pagina's aan reacties van fabrikanten

The table below provides an overview of the overall score each individual IoT product within each of the defined categories. Scoring is based on the conducted assessments of the devices, according to the scripts described in Chapter 2. Devices are scored based on a curated list of security aspects from the testing script, where each aspect contributes a certain amount of points. The overall score is given as a percentage of the maximum possible score. As we noted in Chapter 2, devices should primarily be compared to devices within their own category. A device with a high score is not necessarily "safe". devices with a single critical finding can still have a relatively high score but be insecure at the same time. Establishing a simple and understandable benchmark of safety for IoT devices is very much still an open problem.

Product	Category	Score %	Most severe finding
TP-LINK ARCHER C3150	Routers	**71,0%**	Medium
Huawei B315s-22	Routers	**82,8%**	Medium
Linksys MAX-STREAM EA7500	Routers	**73,1%**	Critical
Asus RT-AC68U	Routers	**78,8%**	Medium
Netgear Nighthawk X4S R7800	Routers	**78,2%**	Medium
VTech Storio Max	Smart Toys	**79,2%**	High
Spider-Man App-Enabled Superhero	Smart Toys	**79,5%**	Low
MAKEBLOCK Codeybot	Smart Toys	**53,8%**	Critical
RC Spy tank met camera	Smart Toys	**45,3%**	Critical
I-Spy Tank met camera - RC Tank	Smart Toys	**43,7%**	Critical
Ubiquiti UniFi Video Camera G3	IP Cameras	**75,5%**	Medium
Foscam C1	IP Cameras	**74,4%**	High
Hikvision DS-2CD2385FWD-I	IP Cameras	**77,5%**	Medium
Nuki Smart Lock	Smart Locks	**69,2%**	High
Danalock V3 Homekit	Smart Locks	**74,5%**	High
Nemef Entr	Smart Locks	**82,5%**	Medium
iBaby Monitor M6	Baby Monitors	**78,7%**	Medium
Arlo Baby babyfoon	Baby Monitors	**85,8%**	Low
Alecto IVM-100 wifi babyfoon met camera	Baby Monitors	**80,7%**	No findings
Nest Learning Thermostat V3	Thermostats	**87,4%**	No findings
Remeha eTwist	Thermostats	**79,1%**	Low
Nefit ModuLine Easy	Thermostats	**78,4%**	Medium

Table 33: IoT Device Score

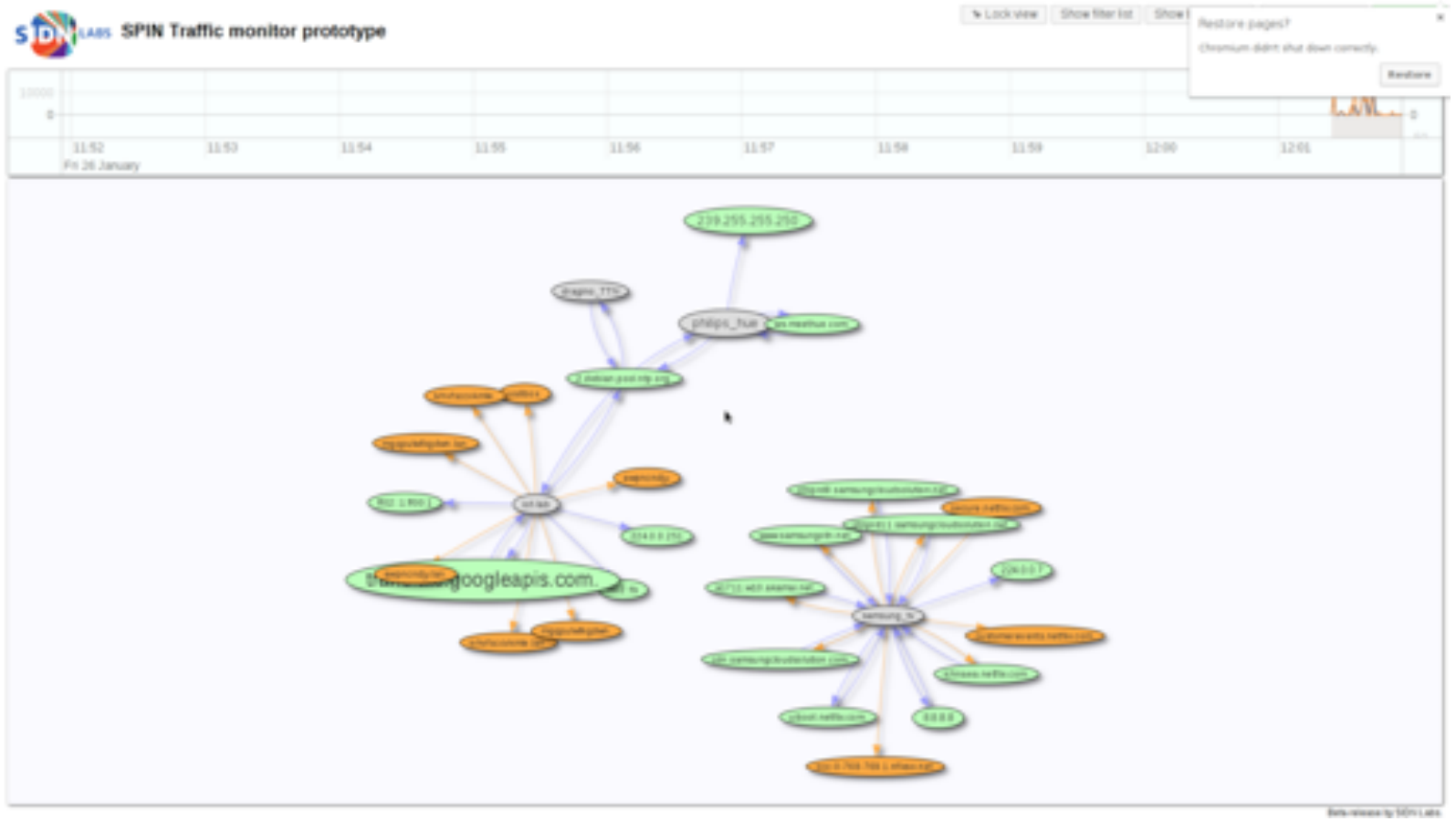
Netwerkbeveiliging

- F-secure Sense
- Fing box
- Keezel
- Roqos

SPIN project bij SIDN

Platform om security- en privacy-aspecten te onderzoeken.

Open-source van belang



Vraag

Welke oplossingsrichting is het meest kansrijke?

A Wetgeving en certificeringen (overheid)

B Concurrentie op beveiliging aanwakkeren (leveranciers)

C Quarantaine (ISP)

D Beveiligingssystemen voor thuisnetwerken (eindgebruiker)

Wat kun je zelf doen?

Wat kun je zelf doen? Ontwikkelaars en fabrikanten

Volg de standaarden en best practices.

Bijvoorbeeld:

- IoT Security Foundation
- Manufacturer Usage Description (RFC 8520)
- Agentschap Telecom ‘Essential requirements for securing IoT consumer devices’
- Privacy by design en default
- Gebruik veilig OS / libraries

Wat kun je zelf doen? Beheerders en ISPs

- Detectie binnen netwerken
- Actief bestrijden
- Samenwerken & delen dreigingen

Wat kun je zelf doen? Eindgebruikers

Doe onderzoek:

- Zoek of er rapportages zoals van Agentschap Telecom zijn over het apparaat dat je wilt aanschaffen

Volg ‘best practices’

- Verander standaard wachtwoorden
- Houd ook IoT-devices up to date
- Internettoegang niet nodig? Laat het slimme apparaat standaard blokkeren
- Of kies bewust voor iets dat niet 'smart' is.

Conclusie

Nog veel uitdagingen op gebied IoT Security

… maar ook veel oplossingen

Zijn er nog vragen?

Volg ons

SIDN.nl


@SIDN

SIDN

Dankjewel voor je aandacht!

De slides komen op
www.sidnlabs.nl

Further reading

https://www.agentschaptelecom.nl/documenten/rapporten/2019/09/25/rapport-digitale-veiligheid-van-iot-apparatuur

C. Hesselman, M. Kaeo, L. Chapin, kc claffy, M. Seiden, D. McPherson, D. Piscitello, A. McConachie, T. April, J. Latour, and R. Rasmussen, “The DNS in IoT: Opportunities, Risks, and Challenges”, IEEE Internet Computing (to appear), https://www.sidnlabs.nl/downloads/49DguF5OpLVw5HCXfROdzW/9c7126fce8ddc80b0850d85f04d64139/The-DNS-in-IoT-Authors-Version-2020-SIDN-Labs.pdf